NPS ARCHIVE
1999.03
ILLYASHOV, O.

DUDLEY KNOX LIBRARY
NAVAL POSTGRADUATE SCHOOL
MONTEREY CA 93943-5101

NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

DEVELOPMENT OF THE INFORMATION INFRASTRUCTURE FOR THE MINISTRY OF FOREIGN AFFAIRS OF UKRAINE

by

Oleksiy M. Illyashov

March 1999

Thesis Co-Advisors: James Emery
Rex A. Buddenberg

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE March 1999	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE : Development of the Information Infrastructure for the Ministry of Foreign Affairs of Ukraine	5. FUNDING NUMBERS
6. AUTHOR(S) Oleksiy M. Illyashov	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT	12b. DISTRIBUTION CODE
Approved for public release; distribution is unlimited.	

13. ABSTRACT *(maximum 200 words)*

The objective of thesis is to determine the needs of the Ministry of Foreign Affairs of Ukraine and design an appropriate information infrastructure. Choosing the best solution for this government organization requires an in-depth understanding of the methods and technologies available and the organizational problems and needs in conditions of the deep economical crisis in Ukraine.

This thesis evaluated existing information systems, and reviewed the current architecture and problems. Research includes a detailed analysis of intranet technology, virtual private networks, secure messaging system and the development of a feasible solution for this government organization.

14. SUBJECT TERMS Information Infrastructure, information technology management, intranet, Virtual Private Network, Network security.	15. NUMBER OF PAGES 116
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

Approved for public release; distribution is unlimited

DEVELOPMENT OF THE INFORMATION INFRASTRUCTURE FOR THE MINISTRY OF FOREIGN AFFAIRS OF UKRAINE

Oleksiy M. Illyashov
Lieutenant Colonel, Ukrainian Air Force
BS, Kiev Military Aviation Engineers Academy, 1983
Ph.D., Kiev Military Aviation Engineers Academy, 1990

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
March 1999

ABSTRACT

The objective of thesis is to determine the needs of the Ministry of Foreign Affairs of Ukraine and design an appropriate information infrastructure. Choosing the best solution for this government organization requires an in-depth understanding of the methods and technologies available and the organizational problems and needs in conditions of the deep economical crisis in Ukraine.

This thesis evaluated existing information systems, and reviewed the current architecture and problems. Research includes a detailed analysis of intranet technology, virtual private networks, secure messaging system and the development of a feasible solution for this government organization.

TABLE OF CONTENTS

I. INTRODUCTION 1

A. PURPOSE 2

B. RESEARCH QUESTIONS 2

C. THESIS OUTLINE 4

II. MFA INFORMATION INFRASTRUCTURE AND NEEDS 5

A. CURRENT MFA INFORMATION INFRASTRUCTURE OVERVIEW 5

B. CURRENT INFORMATION FLOW 10

C. PRIMARY NEEDS RELATED TO THE INFORMATION TECHNOLOGY 11

D. PROPOSED SYSTEM 14

III. INTRANET TECHNOLOGY OVERVIEW 17

A. AN INTRANET BENEFITS AND USAGE 17

1. Organizational Focus 19
2. Intranet as a Tool 20
3. Intranet Uses 20
4. A Decision-Making Tool 21
5. Learning Organization Tool 21
6. A Complete Communication Tool 22
7. Collaboration Tool 23
8. Expert's Tool 23
9. Invention Tool 24
10. Telephone of the next Century 24
11. Intranet Cost Savings Benefits 24
12. Intranet Challenges 25
13. Intranet vs. GroupWare 26

B. Summary 29

IV. INTRANET IMPLEMENTATION 31

A. CHOOSING A SERVER PLATFORM 31

B. CHOOSING A WWW SERVER 33

V. VIRTUAL PRIVATE NETWORK OVERVIEW 39

A. VPN TECHNOLOGY OVERVIEW 39

1. Encryption 41
2. Key Generation and Management 42
3. Certification 44
4. Tunneling 45
5. Interoperability 45
6. Access Control 46
7. Performance 47
8. Network Reliability and Management 47
9. Government Standard of the USSR and Russia GOST 28147-89 49

VI. SECURE MESSAGING 51

B. MINISTRY TO INDIVIDUALS MESSAGING 51

C. PERSON TO PERSON MESSAGING 53

D. SUMMARY OF REQUIREMENTS FOR SECURE E-MAIL SOLUTION 55

VII. NETWORK ARCHITECTURE 59

A. OVERVIEW 59

B. NETWORK DESIGN 59

VIII. COMPUTER SECURITY POLICY AND IMPLEMENTATION 65

A. COMPUTER SECURITY 65

B. THREATS AND CONTROLS 66

1. Physical Security 66
   a. Natural Disasters 66
   b. Intruders 67
2. Software Security 68
3. Information Security 69
4. Environmental Security 71
5. Network Security 71
6. Personnel Security 73
7. Administrative Security 75

IX. LEGACY SYSTEM USAGE 77

A. INTRODUCTION 77
B. THE THIN-CLIENT/SERVER COMPUTING MODEL 78

X. CONCLUSIONS AND RECOMMENDATIONS 81

A. CONCLUSIONS 81
B. RECOMMENDATIONS 83

APPENDIX A. WEBSERVERS QUICK COMPARISON 87

APPENDIX B. VPN FEATURES COMPARISON 89

APPENDIX C. SOME VPN SERVERS FEATURES COMPARISON 91

APPENDIX D. S/MIME PRODUCTS 93

APPENDIX E. PGP VERSION 6.0 FEATURES 95

LIST OF REFERENCES 97

INITIAL DISTRIBUTION LIST 101

LIST OF FIGURES

FIGURE 1. MFA-TO-EMBASSY COMMUNICATION DIAGRAM 7

FIGURE 2. MFA CENTRAL OFFICE NETWORK DIAGRAM 9

FIGURE 3. INFORMATION INFRASTRUCTURE MAJOR COMPONENTS 15

FIGURE 4. MARKET SHARE FOR TOP SERVERS ACROSS ALL DOMAINS 37

FIGURE 5. GROWTH IN INTERNET WEB SITES AUGUST 1995 - DECEMBER 1998 37

FIGURE 6. MINISTRY TO INDIVIDUAL SECURE E-MAIL 52

FIGURE 7. PERSON TO PERSON SECURE E-MAIL 53

FIGURE 8. MESSAGING SYSTEM WITH CERTIFICATE SERVER & PKI 55

FIGURE 9. GENERAL NETWORK DESIGN PROCESS. 60

FIGURE 10. HIERARCHICAL NETWORK DESIGN MODEL. 61

FIGURE 11. MFA OF UKRAINE CENTRAL OFFICE NETWORK DIAGRAM. 64

FIGURE 12. EMBASSY COMMUNICATION AND NETWORK DIAGRAM 64

FIGURE 13. THIN-CLIENT/SERVER ARCHITECTURE [20] 79

LIST OF TABLES

TABLE 1. THE MFA IT DEPARTMENT DEVELOPMENT FACTS 6

TABLE 2. CURRENT INFORMATION FLOW CHANNELS 11

TABLE 3. WEB SERVERS RATINGS 38

I. INTRODUCTION

> "There is nothing more difficult to take in hand, more perilous to conduct, or more uncertain in its success than to take the lead in the introduction of a new order of things."
>
> Niccolo Machiavelli, The Prince

By definition, an infrastructure is something that lays the foundation for something else. The Information Infrastructure (II) for the Ministry of Foreign Affairs (MFA) of Ukraine will lay the foundation for -- and thereby help shape -- new forms of information production, consumption, and interaction between all parts of MFA around the World.

The Ministry of Foreign Affairs of Ukraine is a relatively young and middle-size organization. It was established in 1991 when Ukraine became an independent state after the collapse of the Soviet Union. At that period, there had been employed fewer than 40 diplomats. Now the MFA of Ukraine has approximately 3000 employees in the Central Office and 64 embassies and consulates around the world.

From the technical point of view, the main purpose of this government organization is a search, acquisition, interchange, process, broadcast and storage of different information and data. The quality of this job is very important for Ukraine, because these activities provide the main interface between the Ukrainian government and other countries and international organizations.

Nowadays, the increasing attention to the global information society within international organizations such as the Group of Seven (G-7), the World Trade

Organization (WTO), the Organization for Economic Co-operation and Development (OECD), NATO, and the United Nations Educational Scientific and Cultural Organization (UNESCO) reflects countries' growing awareness that issues in the digital world possess transnational implications. Ukraine is not an exception from this process, but unfortunately, due to the lack of money and because of the rapid organizational growth, the MFA Informational Infrastructure remains undeveloped.

A. PURPOSE

Considering the vital role of the information and communication infrastructure, and realizing that the current telecommunications and information policy have not keep pace with the latest developments in telecommunications and computer technology, the goal of this thesis is develop a project for a feasible information infrastructure based on modern information technology such as Internet, intranet, virtual private network, and secure messaging system.

B. RESEARCH QUESTIONS

The research questions divide themselves into two main categories:

- Problem identification and requirements.

    1. What is the current information technology in the MFA?
    2. What are their primary needs and problems?
    3. How can computers intelligently connect information seekers to sources?

4. How can information access be complete, correct, timely, felicitous, transparent, authentic, authorized, and secure?
5. What architectures can best leverage rapidly changing information environments?
6. How can groups of people and computers cooperate effectively over distributed networks?
7. How should a system security be implemented?
8. How should legacy hardware be used?
9. How should the system be controlled and maintenance?

- Potential solutions.

1. What is intranet technology?
2. What are the advantages and disadvantages of using intranet in the MFA of Ukraine?
3. What kind of software and hardware are feasible for implementing a Web-based information infrastructure?
4. What is a Virtual Private Network (VPN)?
5. What are the advantages and disadvantages of using VPN in the MFA of Ukraine?

C. THESIS OUTLINE

Chapter II provides background information about Current MFA Information Infrastructure, including basics IT needs and problems. Chapters III and IV provides an intranet technology overview and possible application of this technology. Chapter V gives a Virtual Private Network overview and the role of this network for connecting embassies with Kyiv (capital of Ukraine). Questions related to the secure messaging system and different aspects of implementation are discussed in Chapter VI. In Chapter VII, we will discuss Network architecture for the MFA Central Office backbone and a typical embassy. Computer security policy and implementation analysis you can find in Chapter VIII. Chapter IX provides an overview of legacy system and usage problems. Finally, conclusion and recommendation are covered in Chapter X.

II. MFA INFORMATION INFRASTRUCTURE AND NEEDS

A. CURRENT MFA INFORMATION INFRASTRUCTURE OVERVIEW

After 1991, when Ukraine became an independent State, MFA of Ukraine had learned the hard way that dramatically increasing the complexity of the business and size of the organization greatly increased the demand for information throughout the Ministry. Top managers and diplomats received their education and early work experience before the wide-scale introduction of computer technology. In addition, in the Soviet period computers were mostly prohibited in MFA for security reasons. As a result, top managers often fail to understand technology and lack sufficient grasp of the issues to provide appropriate managerial direction.

MFA according to the International Agreements also had to establish a network of direct communications between OSCE[1] capitals for the transmission of messages relating to the agreed measures [1]. To accomplish this task, the Ministry in 1993 created the Operative Communication Department within the Arms Control and Disarmament Directorate. This Department became "de-facto" a computer center for the entire organization without any formal assignment. Only in 1998, this subdivision was reorganized as an independent unit, which has responsibility for the development and implementation of the information infrastructure (II). Unfortunately, the lack of computer specialists (see Table 1.), significant amount of work and deficiency of dedicated financing makes the elaboration of modern IT system very difficult.

---

[1] Organization for Security and Co-operation in Europe (OSCE)

Table 1. The MFA IT department development facts

Year	Approx. # of Computers in Central Office	# of Computer Specialists (Soft/Hardware)	# Of LANs in Central Office	# of Embassies in WAN
1991	20	3/3	0	7
1992	30	0/0	0	0
1993	80	0/0	2	7
1994	110	1/1	3	14
1995	140	0/0	0	21
1996	190	4/2	0	29
1997	210	0/0	0	45
1998	300	2/2	4	64

Due to these reasons and absence of a strategic plan, the development of the IT has an unplanned character. Now the following types of machines are currently in use:

- DOS (i80286, about 10 units);
- Windows 3.x (i80386/486, about 150 units);
- Windows 95/98 (i80486/Pentium/Pentium II, about 130 units);
- Windows NT Server/WS (Pentium/Pentium II, about six units);
- Novell NetWare 3.11 (Pentium, one unit);
- Unix Solaris (Sun, one unit);
- Unix BSD (Pentium, one unit).

Therefore, maintaining such a system with two IT specialists has become extremely difficult.

At the same time, embassies and general consulates had developed information technology systems that provide basic communication functionality (Figure 1).

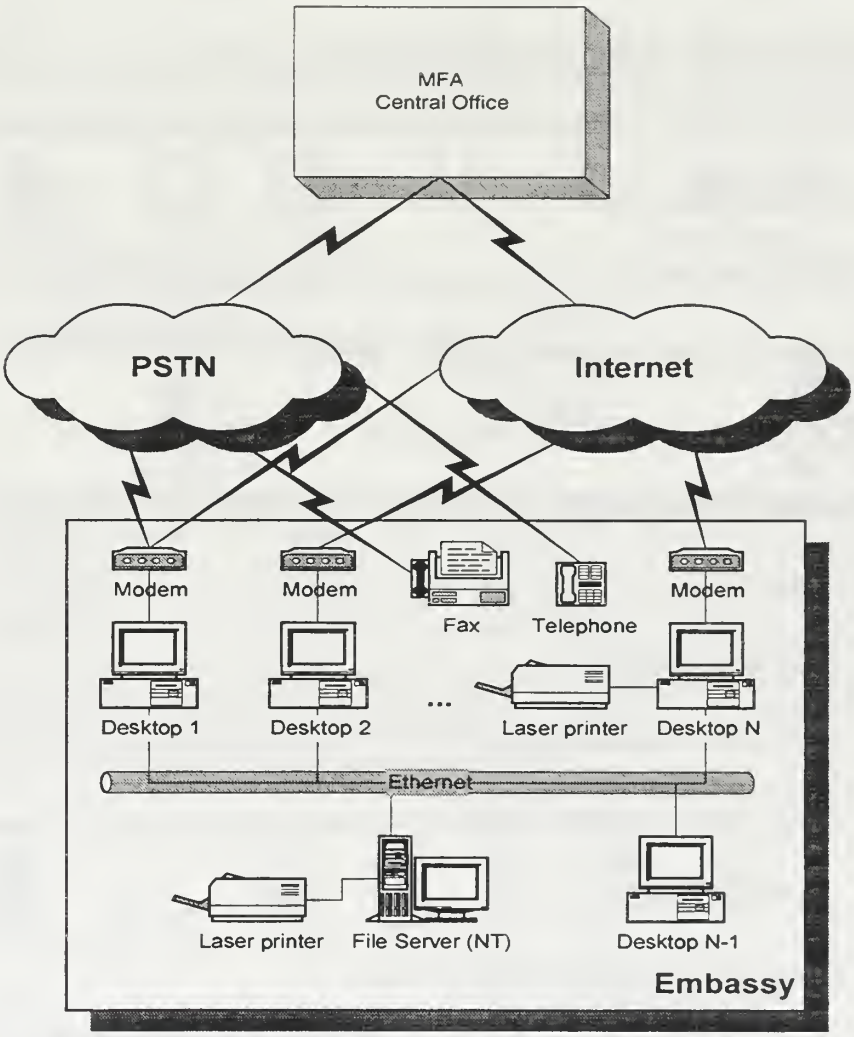

Figure 1. MFA-to-Embassy Communication Diagram

Since the current systems evolved without a Master Plan and without direct IT personnel support, the level of effectiveness, reliability, and security is still very low.

MFA Central Office Network Diagram (Figure 2) shows that Information Infrastructure has problems in different areas:

- Absence of integral computer network (backbone);
- Absence of any LAN in most Directorates;
- The infrastructure is fragmented by multiple "stovepipe" information systems;
- Unnecessary OS variety;
- Single failure point for Internet access (only one line and Web Server);
- Low speed connection with Internet (64Kb/s);
- Not all directorates have Internet access;
- Diplomats do not have personal E-mail even for internal communication;
- Computer security:
  - Absence of a firewalls;
  - Absence of a security policy;
  - System does not provide secure communication between the central office and remote users;
  - Presence of a large amount of modems;
- A lot of obsolete computers in use;
- Hardware systems do not have any backup;

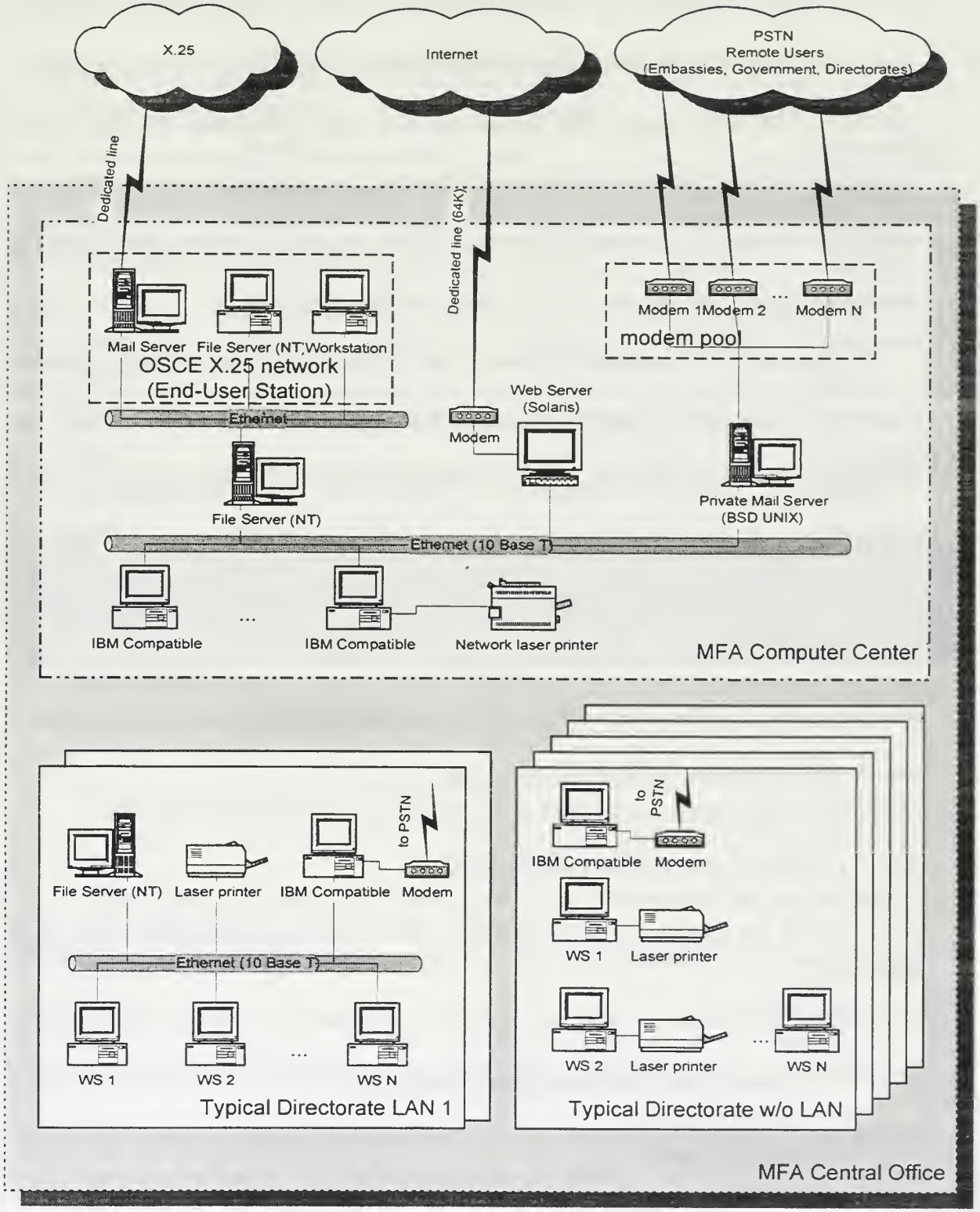

Figure 2. MFA Central Office Network Diagram

The As-Is system cannot meet real MFA information needs. The infrastructure is not planned, architected/engineered, acquired and operated from an MFA-wide perspective. This lack of MFA-wide perspective means that each mission area may develop its own capabilities instead of sharing resources and the solutions may not be interoperable and integrated. Furthermore, existing capabilities are not adequate to meet current changes in mission and policy that are part of new political and fiscal realities.

The scarcity in resources allocated to the MFA in conditions of deep economic crisis in Ukraine has left the organization vulnerable and less prepared to carry out diplomacy in the information age. Flat and declining budgets for MFA resulted in overall erosion of the Ministry's infrastructure, creating critical staffing and training gaps and unmet information technology needs. At the same time, the demand for new information technology and skills are growing exponentially. Therefore, it was impossible to make the investment needed to adequately equip and staff the Computer Center and embassies worldwide with modern information technology.

B. CURRENT INFORMATION FLOW

Today, the information flows between Central Office and Embassies using these channels:

- Phone;
- Fax;
- Private WAN e-mail (using direct phone call);
- Internet (E-mail);
- Diplomatic mail;
- Postal Service mail;

Each of these methods has pro and cons:

Table 2. Current Information Flow Channels

	Channel name	Security level	Cost	Speed	Availability	Type of information
1.	**Phone**	Low	High	Fast	High	voice
2.	**Fax**	Low	High	Fast	High	images
3.	**Private WAN (e-mail)**	Medium	High	Fast	Low	Computer files
4.	**Internet (e-mail)**	Low	Low	Fast	Medium	Computer files
5.	**Diplomatic mail**	High	Very high	Very slow	Low	Paper Documents
6.	**Postal Service mail**	Low	Low	Slow	High	Paper Documents
7.	**Intranet + VPN***	High	Low	Fast	High	Computer files, voice, video

* - future system

C. PRIMARY NEEDS RELATED TO THE INFORMATION TECHNOLOGY

The Ministry of Foreign Affairs is a part of the Government and responsible for providing official relations between Ukraine and other countries and international organizations. Ukraine diplomacy is an instrument of power, essential for maintaining effective international relationships, and a principal means through which the Ukraine defends its interests, responds to crises, and achieves its international goals. The quality of this job has great impact on the country's development in many areas: economy, science, security, culture, and other.

In order to carry out Ukraine foreign policy at home and abroad, the MFA [2]:

- Exercises policy leadership, broad interagency coordination, and management of resource allocation for the conduct of foreign relations;
- Leads representation of the Ukraine around the world and advocates national policies to foreign governments and international organizations;
- Coordinates, and provides support for, the international activities of Ukrainian agencies, official visits, and other diplomatic missions;
- Conducts negotiations, concludes agreements, and supports participation in international negotiations of all types;
- Coordinates and manages the Ukrainian Government response to international crises of all types;
- Carries out public affairs and public diplomacy;
- Reports on and analyzes international issues of importance to the Ukrainian Government;
- Assists Ukrainian business;
- Protects and assists Ukrainian citizens living or traveling abroad;
- Adjudicates immigrant and nonimmigrant visas to enhance Ukraine border security;
- Manages those international affairs programs and operations for which State has statutory responsibility, and;
- Guarantees the Diplomatic Readiness of the Ukrainian Government.

The construction of an information infrastructure to support Ukrainian diplomacy in the 21st century is one of my most critical and urgent objectives. In today's fast-moving, increasingly interdependent, and networked world, Ukrainian diplomats must have modern, secure information technology to respond to world events. Providing this technology to the MFA means deploying the modern information networks needed for rapid, secure Ministry communications worldwide, strengthening information systems security, and ensuring Year 2000 compliance for critical communication and computer systems.

According to the Internet Industry Almanac, there will be over 327 million Internet users by year-end 2000 up from 100 million Internet users at year-end 1997 [3].

The availability of an information infrastructure, which is accessible by all Ukrainian citizens and by all Internet users, can offer significant opportunities to enhance the delivery of Government programs and services.

In order to meet these goals, the Information Infrastructure must provide:

- Information processing and transport services used by Central Office and embassies;
- Support of common (documents flow control, news broadcasting, etc.) and specific (for Consular, Financial Management System, etc.) information services;
- Secure messaging;
- Reliable access to information resources throughout the organization;
- Database management;
- The end-to-end high speed connectivity of all computers within MFA;
- Cost-effective hardware and software implementation;
- High security and integrity level for all parts of the Information system;
- Life-cycle support to all elements of the II;

As we can see, proposed information system must satisfy multiple controversial requirements. The most suitable solution might be intranet or GroupWare systems like Lotus Notes, Microsoft Exchange and Novell GroupWise with security mechanisms located at any layer.

D. PROPOSED SYSTEM

As shown on Figure 3, the Information Infrastructure can be based on intranet architecture within MFA offices and Virtual Private Network over Internet for providing secure connectivity between them. In addition to this, some form of "object security" must to be implemented, where the object of interest to the end user is protected, independent of transport mechanism, intermediate storage, etc. Together, these elements can form MFA's end-to-end and user-to-user capability for information distribution, processing, storage, and display. Wherever feasible and possible, the VPN and intranet should be looked to as main communication path for communicating within the organizational perimeter in order to take full advantage of IT. Consequently, it will improve the efficiency, quality of service and cost-effectiveness of this government organization.

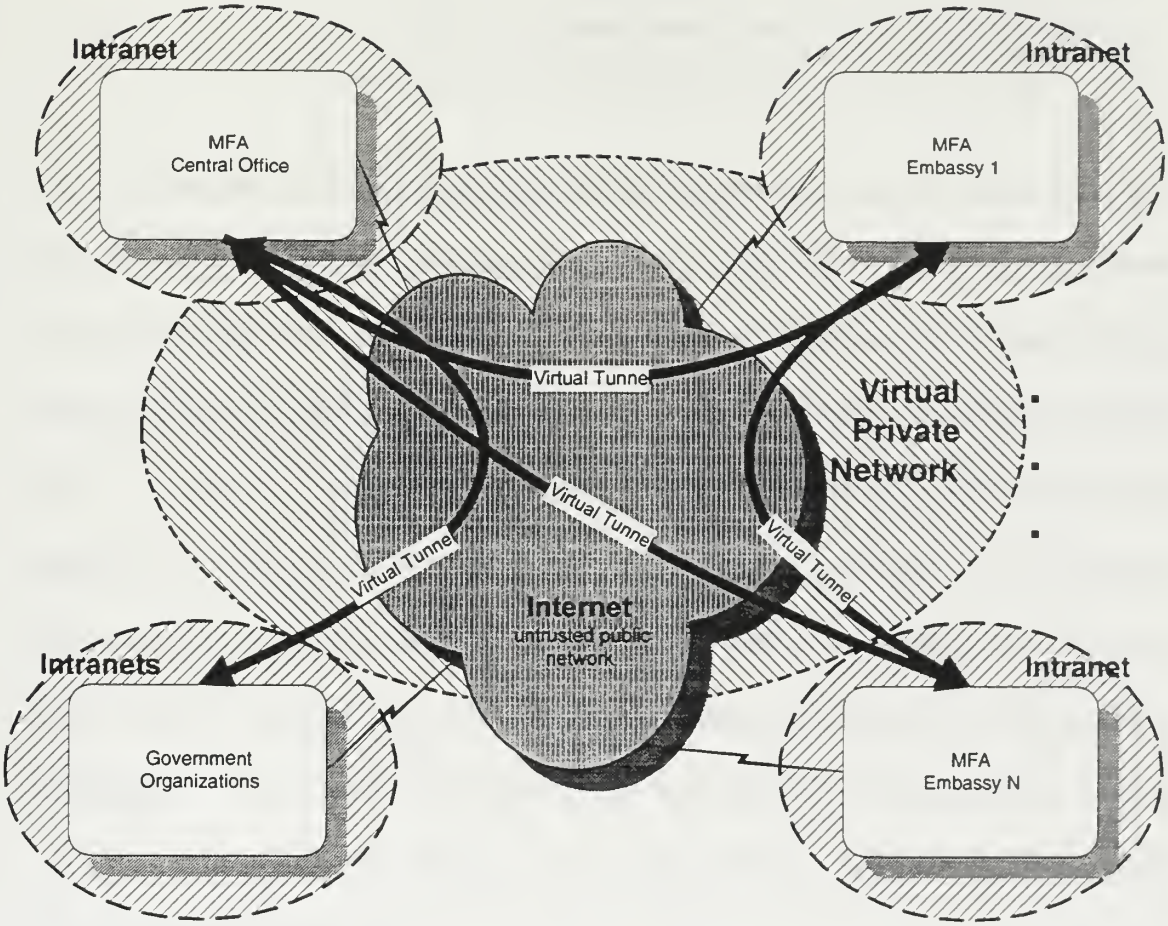

Figure 3. Information Infrastructure major components

The Information System also must provides domestic and worldwide information services for the Ministry, which includes managing a secure global communications network and maintaining the Ministry's central automated data processing system.

III. INTRANET TECHNOLOGY OVERVIEW

> In' tra net - n. 1) a computer network connecting an affiliated set of clients using standard internet protocols, esp. TCP/IP and HTTP. 2) an IP-based network of nodes behind a firewall, or behind several firewalls connected by secure, possibly virtual, networks [4].

An intranet is an internal information system based on Internet technology, web services, TCP/IP and HTTP communication protocols, and HTML publishing. However, the general Internet community cannot access an organization's site. An intranet provides a technology that permits the Ministry to define itself as a whole entity where everyone knows his role, and everyone is working on the improvement and health of the organization. It works by identifying and communicating missions, goals, processes, relationships, interactions, infrastructure, projects, schedules, and budgets on-line, in a single interface everyone uses. In a word, an intranet can represents organization's "intelligence". The purpose of this intelligence is to organize each individual's desktop with minimal cost, time and effort to be more productive, more cost efficient, more timely, and more competitive.

A. AN INTRANET BENEFITS AND USAGE

The intranet is the WAN/LAN, client/server, PC, and UNIX computers that could be used in MFA to do the work, improve efficiency, and communicate with others. The universal and "open standard" offered by HTML and web technology, an intranet system permits offices and employees with different hardware systems to still use the same network. In this way, a diplomat using a PC in the Central Office and another employee

using a Macintosh in an embassy office could use the same intranet system without the need to purchase new and identical computers. With the intranet, MFA employees will have access to all the information, applications, data, knowledge, processes, etc. available in the same window, or the same browser.

To understand the true power of web technology, we need to stop thinking about it as strictly an Internet tool and start evaluating it on its own rather impressive merits.

Today web technology already offers:

- Inexpensive client and server software.
- An intuitive, document-based GUI interface (reads like a book, a menu, or a guided tour with full color in-line graphics).
- Requires no training (just point and click on interesting topics).
- Retrieves virtually any document type on-line (by reading document extensions and spawning external viewers, when necessary).
- Supports multimedia (by retrieving and playing sounds, video, and other multimedia objects).
- Supports imbedded hypertext links to local or remote documents.
- Supports hypertext areas within graphics (e.g., customized push buttons and clickable maps).
- Supports compound documents and reusable images (the newest trend in document architecture).
- Supports SQL queries or other interactive retrieval, display, and updating of database information.
- Supports corporate-wide standardization of on-line interfaces.
- Supports retrieval and display of reports generated by external applications.
- Supports on-line forms, data entry and other two-way interactive communication between users and computers.
- Supports e-mail applications.
- Supports the automatic spawning of shell scripts, batch files, or operating system commands.
- Capable of spawning remote (telnet or 3270) sessions and running remote applications for display on the local screen.
- Supports automatic downloading or transfer of computer files at the click of a button.
- Supports user authentication and encryption schemes.
- Supports on-line real-time commercial transactions.
- Automatically provides feedback on system usage.

- Supports Internet services like Gopher, Archie, and Veronica, even on local networks.
- Supports a wide variety of search engines, with rank-ordered, clickable, automatically hyperlinked search results.
- Supports centralized or decentralized document management philosophies.
- Allows "democratization" of document publishing and organization-wide distribution of documentation responsibilities.
- Supports on-demand printing of desired documents on local or remote printers.
- Non-proprietary, platform-independent, open document architecture based on ISO standards.
- Client-server architecture.
- Consistent viewing on any resolution monitor (user can adjust fonts locally for better viewing).
- Works equally well on standalone computers, local area networks (LANs), wide area networks (WANs), or the global Internet.
- Works on all major desktop-computing platforms (UNIX, Mac, PC, etc.).
- Integrated into popular computer operating environments (e.g., Windows NT, Mac, and Windows 95).
- Works in any commercial network environment supporting TCP/IP [5].

As we can see tools, like Mosaic, Netscape, and Internet Explorer will become the document-based equivalent of the telephone in the 21st century.

1. Organizational Focus

The intranet provides an opportunity to define MFA as organization and display it for every employee to see. If everyone knows what the Ministry stands for, what the organization's strategic vision is, what the governmental guiding principles are, who the allies and opponents are, then they can focus more clearly on what his own contributions are to the organization. Every directorate can constantly refer to the central messages and develop his own supporting sites accordingly. Use the Web as an information, communications, and project-management tool across the Ministry.

2. Intranet as a Tool

We can think of an intranet as a high tech instrument, providing with a set of tools for almost every function within organization. For the future successful operation, MFA of Ukraine must rely on information, knowledge, and intelligence to create high quality services for the country. Information is power. In the past, it was always difficult to get access to it. Either we could not get reliable information, or we could not get it on time. Now, information is managed directly at the desktop with no particular worry about platform or software compatibility.

With an intranet, any user, at any level, can publish information. This makes information reliable because it comes from the source. The individual can serve the information that can be read in any browser, and make itself linkable to any other server. This linkage creates process flow within organization and we can secure information and share information in the best way we see fit. With intranets, everyone in the Ministry can access information, knowledge and organization intelligence and design it in any way that improves business models.

3. Intranet Uses

Intranets can be used for many different functions within organization. Applications that the Ministry and embassies have been using for years are finding their way to the Intranet. Uses include executive decision support systems (DSS), consulate and visas support system, financial systems, online analytical processing (OLAP) applications, personal productivity applications, document management systems, and

residents and non-residents support and help desk applications. The list just goes on and on.

4. A Decision-Making Tool

The intranet may link together all of the information in the MFA. The information can be either pre-determined or we can use interactive forms or report writers to prune and graft information to help diplomats to analyze political trends or other country behavior. The Ministry can share results with other government organizations, embassies, clients and partners, and modify political decisions accordingly. Templates and common look and feel come included. With a sophisticated web-searching tool, diplomats need not sift through long pages of information to get what they want. They can just key in a few keywords, and necessary information will be served to them like a meal. Such a system may be useful for government delegations that work away from an embassy. Using Internet as an access medium, they can get the informational support in real time from any source, internal or external.

5. Learning Organization Tool

When information can be pulled instantly, decision-makers are able to analyze political processes, economical opportunities, and national goals much faster. It follows that more employees can become decision-makers. International treaties and agreements may be managed more efficiently. Communication is opened up to include anyone related to any part of a work. International requirements and laws are documented and

adhered to. Development occurs in a shared electronic development space, rather than between meetings, telephone calls, and individual schedules. The organization that shares information learns together, improves together, and creates a more intelligent structure and behavior.

6. A Complete Communication Tool

Integrating all the Ministry's communications, all departmental communications, all group communications, and all individual communications into a place provides up-to-date, quality, instant information to anyone in the organization, whenever and wherever wanted. From one single place would easily allow everyone in the Ministry to get any information from the executives, human resources, politics, international organizations, science, economy, finance, operations, and facilities. All the hundreds of laws (national and international), documents, press-releases, notes, software, and training materials became accessible on-line. These resources will be available to everyone 24 hours a day. Diplomats can communicate with anyone who produces this information, improving on its presentation or content with knowing where the information came from, when it was generated and how it relates to other information. Employees can send and receive secure e-mail messages and documents on the Intranet. By using the Intranet, document transfer and e-mail messaging are not exposed to the general Internet community. These secure and confidential communications are yet another aspect of an intranet that provides innumerable benefits to the users and organization alike. By using Virtual Private Network, diplomats can expand intranet over the globe. The Ministry can

use Voice over IP technology and save a lot of money, especially on international telephone calls. The Intranet is a powerful communication tool.

7. Collaboration Tool

Productivity of work will significantly improve when an easy to use, easy to learn, powerful tool for collaborating, project managing, data collecting, and managing knowledge and information is handed to everyone in a networked Ministry. This tool empowers people to put their best foot forward, proudly displaying their quality jobs, official messages, internal services, technical procedures, processes, and departmental goals in a place where anyone who subscribes can access them. IT also encorages collaborating with each other without wading through e-mail, or playing telephone tag sessions, or missing chance to input at a meeting. It will be possible to organize forums where people with common interests meet and hash out issues, until the best possible solution is achieved. Then, we can add audio and video conferencing, electronic white boards, single document sharing -- giving us a collaborative tool, the Intranet.

8. Expert's Tool

With intranet any diplomat or specialist may be linked to real-time, on-line web sites that provide support by experts. They can share documents, archives, rules, problems, analysis, and bottom line information about any topic, and get any important information from those who know best and have spent innumerable hours researching, thinking, and putting ideas into action.

9. Invention Tool

Any employees can find information when they needed it, and available to cut and paste it into their documents, presentations, messages, or reports. People will save a lot of the time not reinventing the wheel. Instead of information stored in filing cabinets, desks, garbage cans, and huge piles on desks, information is available on-line for re-use by anyone working on similar topics. Everyone in the organization can tell the same official opinion and position!

10. Telephone of the next Century

The intranet is a tool that has already become a utility in many companies, much like the telephone. Using it, we are empowered to accelerate life cycles, to focus on expert information, to improve services, to get a hold of anyone in the organization. The Intranet will allow individuals to create their own web pages, groups sites, departmental sites, and rule a knowledge environment in which individuals within the organization know who they are talking to, what they represent, and how they fit into the organization. The level of interaction becomes more intelligent and more streamlined to government goals, and national missions.

11. Intranet Cost Savings Benefits

One of the most obvious benefits of an intranet is an actual bottom line money saving. An organization using an intranet system can realize both hard and soft savings:

- Reduced costs - printing, paper, software distribution, mailing, order processing;

- Reduced telephone support expenses;
- Easier and faster access to official government and technical information;
- Easier, faster access for remote locations;
- More thorough research base;
- Easier access to colleagues' data/research efforts;
- Increase in accuracy, and timeliness of information;
- One consistent interface to learn and use;
- Available information is visible;
- Reduced information searching time;
- Reduced setup and update time;
- Reduced documentation costs;
- Reduced support costs;
- Reduced redundant page creation and maintenance;
- Faster, cheaper information creation;

When we consider the intangible factors of these costs, particularly in the costs of paying employees to perform tasks which can be eliminated or substantially reduced, it is easy to see the soft cost savings value of an intranet as well.

12. Intranet Challenges

Intranet technology has not only benefits, but also challenges.

Potential challenges:

- Users education and training;
- Possibly on multiple platforms;
- Security;

- Bandwidth;
- Scalability;
- Manageability;
- Measurement of paybacks;
- Getting/keeping skilled Webmasters, info designers;
- Ongoing maintenance;

13. Intranet vs. GroupWare

Another software solution that can meet Information Infrastructure goals is GroupWare system like Lotus Notes, Microsoft Exchange and Novel GroupWise. The bottom line difference between a WWW server and "collaborative" computing solutions such as Lotus Notes is design philosophy. Designed as a proprietary system in an era lacking widespread connectivity, Lotus Notes uses a proprietary database structure that replicates data and does not provide quick access to the remote databases. A WWW server, however, was designed to take advantage of the Internet's worldwide computer network; it eliminates the need to replicate databases by providing users with easy access to source data.

Another important difference is that a single WWW server platform can support internal and external applications for both internal and external information sharing on the Internet. Lotus Notes, on the other hand, is mostly an internal application.

Since the intranet takes advantage of WWW open-standard technology, it offers a great starting point for the Ministry to disseminate information within the organization

efficiently and cost-effectively. Initial WWW startup costs and commitments are very low, with a minimal initial investment or training. For example, an investment of less than $1K is estimated for site development (cf. multiple $10K commitment for Notes), a dedicated infrastructure or staff is not required, and it is extremely easy to migrate existing content to HTML.

According to a recent research study, the average corporate investment in a Lotus Notes implementation is $245,000, with an average payback period of more than two years. Eighty percent of the respondents to this study targeted a single application. WWW applications can be fully developed and deployed for $10K or less. (Source: International Data Corporation).

The WWW enables users to centralize their information resources in a single point-and-click environment -- the browser -- which is available on a variety of client platforms (PC, Mac, Unix, etc).

The use of client browsers with one standard Window interface offers easy integration with other applications, such as electronic mail, faxes, calendaring, videoconferencing, and hot links within messages. As a single interface to a variety of information sources, the browser is cost-effective, highly efficient, and very easy to use.

While commercial browsers are available as fully functional freeware, the price for Lotus Notes Express is $100 per user, with the full Notes client priced at $155.

Unlike the highly technical Notes environment, the WWW server can also be easily managed by "content creators" rather than IS professionals. The WWW point-and-click environment allows non-technical directorates like Consular or Political Analysis

and Planning -- rather than the Computer Center -- to manage, contribute and update WWW content. This shift of responsibility helps reduce development costs, and enhances productivity by enabling the technical support staff to focus efforts on running the computer systems instead of maintaining server content.

It is less expensive to develop content for the web than for Notes. A wide variety of third-party content tools are available for the WWW server development, while the few Notes content development tools are those provided. Since familiar tools, such as Microsoft Word, can generate HTML code, support staff rather than high-level, technical experts can easily create WWW content.

Content can be easily accessed by browsers on any platform, in any location. Unlike with Notes, data distribution is in real-time, on an as-requested basis, over a public (or private) network.

A WWW server can be easily integrated into an existing environment. For example, Cold Fusion or Visual Café Pro can easily connect the web browser to any ODBC-compliant databases to access a variety of external, pre-existing data sources.

Authorized employees can easily access the WWW server remotely, after being authenticated, and download only the specific information required. This reduces expensive line charges ($1.5-$2 per minute, in the case of a direct international telephone call). For embassies with existing connections to the Internet, the incremental cost is virtually zero.

The WWW can be adapted easily to multi-media applications. For example, video is an easy extension to the basic WWW platform, while video for Notes is an

expensive one-way (no conferencing) proposition ($2,700 for the server license + $120 per client). On the WWW, using publicly available free or inexpensive utilities (Net Meeting, Internet Phone, etc.), the MFA can deploy bi-directional desktop videoconferencing relatively inexpensively.

In sum, startup, training, ongoing management, and updating of web applications cost significantly less than that for the Notes installation. WWW applications broaden the reach of a "team" application to more than an enlightened highly technical few.

In current conditions with limited money and IS professionals, MFA does not specifically require "collaborative" GroupWare applications, but instead needs an easy, effective, fast, and inexpensive way to share information for an effective business.

The benefits offered by the intranet include cost savings, minimal training, single source of data, links to outside data sources, and easy management and delivery of information. When we weigh these advantages, we can see that, for the Ministry of Foreign Affairs of Ukraine, they far outweigh the benefits of the information- handling capabilities of collaborative-GroupWare tools such as Lotus Notes.

B. SUMMARY

To summarize, the intranet may be the future of MFA Information Infrastructure. All future computer applications will be built and delivered on this universal foundation.

The intranet is already functioning in the thousand different organizations around the world. Therefore, it can be used as an information superhighway for employees who want to publish and distribute data and documents instantly across the Ministry.

Intranet is a relatively easy add-on to the existing TCP/IP networks. Much of the software is available initially as freeware or shareware.

IV. INTRANET IMPLEMENTATION

There are two main areas for intranet implementation – organizational and technical. In this document, we will discuss only the technical aspect of this problem.

A. CHOOSING A SERVER PLATFORM

Creating an internal web site is a low-cost, minimal risk investment. It is easy to implement, with little training or equipment required. The basic system configuration consists of a server hardware platform / operating system and WWW server software. In our case, the main part of the investment must be in the creation of the LAN and client PC installation. The LAN deployment problem has a well-known solutions and any modern technology like ATM or Fast Ethernet can be suitable for this task. For our purpose, we will assume that MFA already has client PCs in place.

As a server platform, the requirement is server hardware with sufficient memory and disk space to run Windows NT, Windows 95, and/or a UNIX system platform, depending on our preference and in-house expertise.

Several factors will come into play when deciding which platform we should use to build MFA intranet. Several major areas should guide us in the decision making:

- Existing infrastructure;
- Personnel skills;
- Ease of administration;
- Price;
- Scalability;
- Security;

- Support.

Chapter II shows that most computers in the Ministry are PCs with MS Windows. It is very unlikely that in the future the Ministry will deploy UNIX computers for everyday work like word processing, web browsing and so on. Conversely, we probably would not want to install a UNIX box in an exclusively Windows environment. The current IS personnel cannot provide sufficient UNIX administration and support level.

System administration is a big part of maintaining an intranet. Administrators are responsible for such things as adding new users, installing applications, maintaining security, and seeing to it that the intranet is kept up and running. In this area, NT wins easily. NT combines an intuitive GUI with powerful tools in an easy to use point and click environment. Installing new software on NT usually involves running a single setup program that guides the administrator through the setup process. UNIX on the other hand, could be a more difficult for the administrator (especially for those who are new to UNIX). Although some versions of UNIX have a GUI, most administration is done from the command line, making it difficult to visualize the process. However, one of the advantages of the command line is case of remote (over network) administration. Remote administration NT computers require special software. Setting up software applications on UNIX can also be a real problem.

Another factor is cost. Because NT is relatively inexpensive, it stands to gain a larger market share than do more expensive UNIX operating systems.[2] Similarly, NT is

---

[2] However, some of UNIX versions are free (Linux, FreeBSD) and can run free web server program as Apache, AOLServer and other (see Appendix A).

designed to run on inexpensive PC platforms while the majority of UNIX OS's are designed to run on larger and more expensive workstations and mainframes. Cost may not be an issue for larger firms like Sun and IBM, but for MFA of Ukraine, the differences are important.

Actually, in same cases, Unix has advantages, and some experts prefer UNIX-based system. It offers a variety of vendors (no threat of a monopoly), scalability, remote administration, remote computing, multi-user capabilities, large palette of software resources (especially for the servers), vendor independent standards (POSIX), control of users' disk usage (unlike NT 4), and cannot be crashed by viruses written 10 years ago for DOS computers [7]. Even so, NT seems to be a better solution for the MFA of Ukraine because we need to keep uniformity among OS's on servers. Otherwise administration cost and problems will be much higher.

An increasing number of organizations (for example, US Navy with IT21 program) are opting for Windows NT in the development plans today, because of it open architecture and ease of use.

B. CHOOSING A WWW SERVER

WWW servers provide an efficient, single-point source of information. Pointers to information can be preloaded into client PC or Macintosh browsers, with links programmed into the documentation. High-level subject lines -- Political, Consular Support, Protocol Information and other -- provide an easy-to-use roadmap to further detailed information. Web server software facilitates management of internal WWW

presence on the intranet. The right WWW server software solution will give us the functionality required to setup and manage Home Pages, develop WWW content based on Hypertext Markup Language (HTML), perform text searches, and integrate with internal corporate databases or BackOffice applications.

On the client side, each user who plans to access the internal WWW site will need a 486 or Pentium-PC (or notebook) with a minimum of 8MB memory to run client browser. Nowadays the best client browsers are free and can launch a variety of applications, access disparate databases, retrieve information from across the Internet, etc.

WWW content software is also required to generate HTML code so users can add HTML tags to convert their current documents into WWW documents. It is very easy to develop content for the web using MS Office 97 software or one of the many inexpensive, third-party HTML authoring tools and editors. Depending on real organizational requirements, we can also take advantage of numerous other commercial tools that are also available, including text retrieval/indexing software, links to database management systems, and server configuration or management tools.

Since the WWW server serves as the cornerstone for managing the WWW site, it is important to determine the type of functionality required. The following questions provide guidelines for making the right choice:

- Are there special resource or configuration requirements?
- Who will be installing the WWW server? How important is easy installation?
- What type of search engine and text retrieval is supported?

- What Internet proxy support (e.g. HTTP, GOPHER, FTP) will MFA need? Does the WWW server support these protocols?
- Will multiple Home Pages be installed on the same server? If so, how easy is it to manage and administer? Is remote administration a requirement?
- Are HTML tools supported for application development?
- Who will be responsible for managing the content? Will this be someone technical or non-technical?
- What kind of database will support MFA employees access to organizational databases?
- What are security requirements? For example, will it be necessary to protect highly confidential information and restrict access to certain workgroups? If so, what types of access controls can the WWW servers define?
- What type of training, documentation, and ongoing support is available?

Appropriate Web Server must support following requirements:

- Running on Windows NT,
- Can write to multiple logs,
- Supports Virtual Servers,
- Comes with a SNMP agent,
- Supports SSL v. 3,
- Integrated certificate server,
- Can require password (user authorization),
- Remote maintenance,

- Includes full source code for server,
- Has a search engine.

According to the "WebServer Compare", which is a service of internet.com [8], there are five matches:

- Apache 1.3 by The Apache Group,
- Internet Information Server 4.0 by Microsoft Corp. ,
- Lotus Domino Go Webserver 4.6.1 by IBM,
- Netscape Enterprise Server 3.5.1 by Netscape Communications Corp.,
- Oracle Web Application Server 3.01 by Oracle Corp.

The Netcraft Web Server Survey [9] provides a survey of Web server software usage on Internet connected computers. The most popular Web servers are Apache and Microsoft IIS. In the December 1998 survey received responses from 3,689,227 sites. (see Figure 4 and Figure 5)

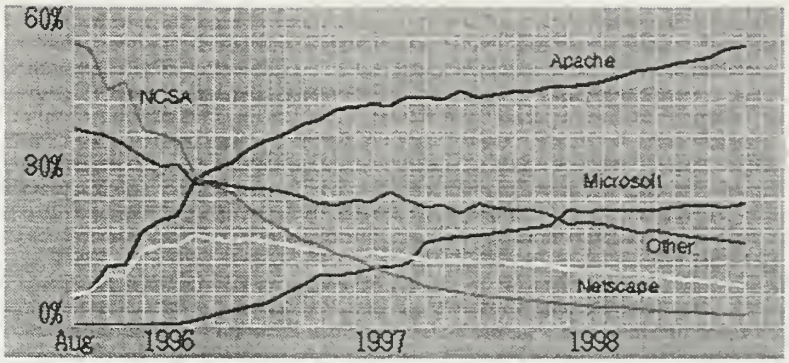

Figure 4. Market share for top servers across all domains

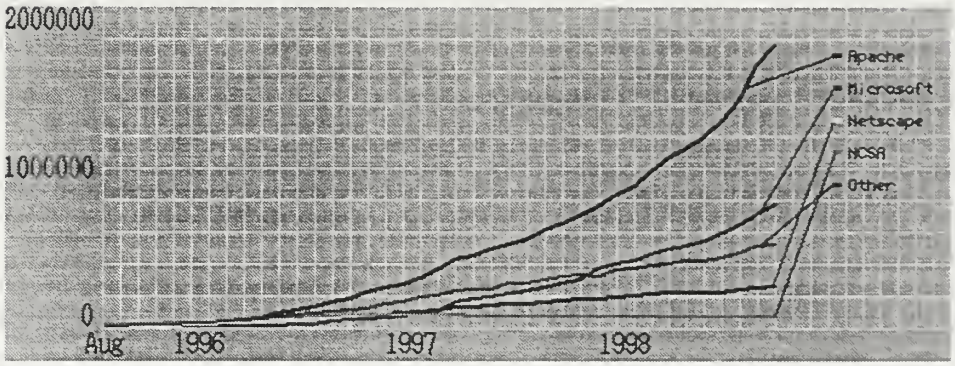

Figure 5. Growth in Internet Web Sites August 1995 - December 1998

It will be feasible to choose Internet Information Server v.4 from Microsoft or Apache from the Apache Group as primary candidates for Web server software.

Based on in-depth reviews and Web server analyses made by Mecklermedia Corporation [10], we can compare the ratings of these software products (rating range from one to five, one means bad, two -- better, etc.). (Table 3.)

Table 3. Web Servers ratings

Ratings	**Apache 1.3.4**	**IIS 4.0**
Reliability	5	4.5
Performance	5	4.5
Ease of use	3	4
Tech Support	4.5	4

These ratings and detailed comparison of the features (Appendix A) show that Apache has more advantages; its market dominance is not a mistake. High reliability and performance make Apache a number one candidate for the deployment as a server platform.

V. VIRTUAL PRIVATE NETWORK OVERVIEW

A. VPN TECHNOLOGY OVERVIEW

The Internet is an almost ideal media for information retrieval and exchange between MFA offices around the world. It is cost-effective, easy to use and accessible in every capital city of the world. The Internet is a shared media, to which millions of users are connected, and there are very few regulations on how it is to be used. Moreover, just as these traits make the Internet an attractive method for honest activity, so too do they make it a very efficient medium for devious tasks such as data tampering, eavesdropping and theft.

The widespread hacks have generated a demand for turn-key solutions capable of creating secure Virtual Private Networks: cost effective multi-site networks built on public backbones. The IT community has responded, and the results are emerging VPN technologies that incorporate network encryption, access control, certification and network management.

Not surprisingly, secure VPNs represent one of the hottest areas of the international networking market. Spending on VPN products, systems integration and ISP services is projected to grow from an estimated $205 million in 1997 to $11 billion in 2001, according to a 1997 report by San Jose, Calif.-based Infonetics Research, Inc. [11].

VPN systems enable distributed private networks to communicate securely with each other over untrusted, public networks. They encrypt transmitted information with

complicated algorithms to hide sensitive data from unauthorized access. The general process is as follows:

1. A protected host sends clear traffic to a VPN kit (the source device) located at the point of connection to the public network.
2. The source device examines the data according to rules specified by the network manager, securing the information or allowing it to pass unaffected.
3. When data protection is required, the source device encrypts (encodes) and authenticates (attaches a digital signature to) the whole packet, including the transmitted data as well as the source and destination host IP addresses.
4. The source device then attaches a new header to the data, including the information that the destination device requires for security functions and process initialization.
5. The source VPN kit then encapsulates the encrypted and authenticated packet with the source and destination IP addresses of the destination device, or devices. This results in a virtual tunnel through the public network.
6. When the data reaches the destination device, it is decapsulated, its digital signature is checked and the packet is decrypted.

The result of the tunneling process is the scrambling of transmitted information to make it legible only to its intended recipient. Creating a secure VPN usually requires devices capable of performing the different scrambling tasks as well as guidelines that determine what communications traffic is encrypted and what is not. In order to address these issues, secure VPNs work according to predefined rules and operate automatically and transparently to the user. Employees residing in the VPN work normally. They can

go on line, send email to other diplomats and specialists or download documents, and the VPN determines which of their tasks are to be conducted secured and which should continue in the clear. Full privacy is maintained, communications costs are reduced, but efficiency and employee output remains unchanged.

For MFA, there are a number of options in setting up a VPN. We can choose between software add-ons to routers, software firewalls with encryption patches, software VPN systems, or dedicated hardware VPNs. (Appendix B and C)

1. Encryption

Encryption is the starting point of any VPN solution. One of the essential differentiators between effective and ineffective VPNs is the use of well-established encryption algorithms and strong encryption keys. Several techniques are suitable, although the symmetric GOST 28147-89 (for former Soviet Union countries) or DES/3XDES (for the USA) algorithms are mostly used for payload encryption while the asymmetric (also known as Public Key) RSA and Diffie-Hellman algorithms are popular for key exchange. The above mentioned encryption keys are well known and tested, and libraries of information have been devoted to their reliability and efficacy.

Encryption is a difficult process, and when dealing with the quantities of information transferred across modern networks, CPUs can be confronted with staggering workloads. It is not surprising, therefore, that the secure VPN market is heading towards dedicated hardware solutions over their software equivalents.

Hardware focussed on security-only functions is better able to cope with the strains involved in encryption and authentication and, as a result, can provide powerful security features without significantly affecting network performance.

2. Key Generation and Management

Since encryption algorithms are well known, the strength of the encryption process comes down to the key used in encrypting and deciphering transmitted data—the well-kept secret shared by the component machines of the VPN— and the protocol used in the key management process.

The security of the VPN's encryption methodology is a combination of the following factors:

1. Key length: In general, the longer the key, the tougher to break. Today, a key length of less than 56 bits (when using the DES algorithm) is considered insecure.
2. Key exchange mechanism: As mentioned above, keys are the common secret upon which the whole encryption process strength is based. Key exchange, therefore, should be based on well-established algorithms (e.g., Diffie-Hellman for encryption and RSA for signature) as specified in strong key management standards. Today, the IKE protocol (rather than Simple Key Management for Internet Protocol, or SKIP), is the preferred method. The primary advantage of IKE over SKIP is the former's ability to negotiate with a number of different encryption keys. This prevents unrecognized messages

from being sent outside protocol guidelines, thus providing greater robustness and enhanced security. In addition to standard methods, MFA has privilege to use diplomatic mail for the key distribution with a high level of security. Recordable CDs with a capacity of 650 MB of data (or DVD-RAM) can be used even for the implementation a one-time pad protocol.

3. Rate of key exchange: As a rule, the more frequently a key is automatically exchanged, the more secure the encrypted data. VPN solutions which use manual (by diplomatic mail) key exchange could be insecure, as users may not always remember to change keys or may choose not to bother with the often cumbersome manual key exchange process. Similarly, a key exchange only at the end of a session is unreliable, as large amounts of data can be accessed if the key is compromised.
4. Key generation: In principle, the use of true random keys ensures the highest levels of security. With real random numbers as the bases for encryption keys, it is impossible to know or predict the structure of past or future keys. The best method of key generation is hardware (usually, a noise diode). Software-based key generation, in contrast, use known algorithms, which, given enough time and money, can be cracked.

3. Certification

Certification is the registration and identification of VPN components. It requires establishing well-defined secrets between a centrally controlled Certification Authority and any VPN device. A poorly designed and implemented certification process, such as a password, may result in an "easy to join" VPN to which unwanted entities may connect as members.

The first step in adding new gateways to the VPN involves the transfer of secret information in a simple yet secure way (diplomatic mail). This process must be carried out with extreme caution as no encryption system has been established. The use of secured hardware tokens is recommended for this preliminary certification phase, as they provide a secure means of loading the security information, off line, into the new gateway.

Once the transfer of the initial secret is complete, the rest of the certification process, as well as the distribution of the new certificate to all existing VPN gateways, should be done secretly and quickly in order to allow for the fastest possible set-up and operation. It is necessary, therefore, to employ a fully automatic and secure (encrypted and signed) certification process. VPN solutions which send the initial secret unprotected message over untrusted networks are ineffective and are not secure, and those which involve the manual input of new units into an existing data base involve significant costs when expanding the VPN.

4. Tunneling

Tunneling is the encapsulation and encryption of entire transmitted packets. An effective tunneling mechanism hides the networking data in addition to the application and payload layers, i.e. from layer three and above (referring to the OSI model). A VPN solution, which only encrypts the payload, is not sufficiently secure, as a multitude of information is obtained by analyzing networking parameters.

Layer three tunneling is also advantageous from a scalability standpoint. As IP's dominance continues to strengthen, greater will the need become to protect all varieties of IP applications over IP backbones. Layer three encryption is application and network independent. It can be applied to any form of routable communications (voice, video, and data), thus providing an effective scalability pathway.

5. Interoperability

The emerging Internet Protocol Security (IPSec) standard [12], as created by the Internet Engineering Task Force (IETF), is becoming the international standard for virtual private networking. With IKE key management at its base, IPSec has created a secure means for interoperable security. It guarantees that encrypted information is protected on its way from one network to another, while also allowing partner organizations to link their respective VPNs together, even if their encryption systems were manufactured by different vendors. VPN solutions that are not IPSec-compliant (i.e. not interoperable with

the industry standard) will prove more expensive in the long run and will limit a government VPN's growth potential.

6. Access Control

Encryption without effective and efficient access control (i.e., "firewalling") is but half the VPN technology, for Internet-based VPNs require defense mechanisms from those who would seek to hack their way into the networks from the Internet. Two issues of primary importance in evaluating the strength of firewall features are the operating system on which the system runs and the methodology used:

1. Operating system: Software-based solutions are built on well-known operating systems, such as UNIX and NT. Hacking methods for targeting bugs and security holes in these operating systems are readily available on the Internet. Hardware-based solutions, in contrast, employ real time, hardened operating systems that do not fall victim to popular hacking methods. The strength of the hardware VPN's OS translates into better security throughout the network.
2. Methodology: The effectiveness of a firewall is linked directly to the scope of its inspection technique. Access control systems must be able to analyze all levels of incoming and outgoing data, including the content payload itself. Content analysis gives the ability to look inside data flowing through the VPN system. It can weed out commands from sessions, such as FTP "get" or "put" instructions, thereby providing limited access to areas of a VPN but preventing attempts to alter stored information.

7. Performance

Effective VPN solutions must be able to operate at true wire speeds. Those that do not will form a bottle neck in the communications environment and will prevent the transfer of information. The performance issue becomes even more crucial when more complex encryption algorithms are used (e.g., Triple DES). Hardware-based solutions, which are fully dedicated to the task of generating and processing encryption algorithms, are better suited to coping with longer encryption algorithms, and therefore provide a communications infrastructure better able to adapt to the needs of the future.

8. Network Reliability and Management

A VPN is a networking solution. As such the basic requirements of other networking media must be met by a VPN.

1. No single point of failure: This important characteristic is achieved through the incorporation of automatic backup gateways (redundancy) into a VPN. Mission critical networking applications require redundancy options for worse case scenario planning. The recent failure of a MFA communication computer and its impact on information flow clearly demonstrated that the unthinkable could and will take place. In order to protect a VPN from the potentially disastrous effects of an office fire, for example, it is important to include "hot backup" topologies within the network architecture. In addition, VPN devices must be configurable to distribute security functions throughout the network. Centralized session or key distribution authorities are incompatible with mission critical communications.

2. Network management: the over-riding concept behind VPN communications is the use of security technologies to increase connectivity. Capable security features in themselves, however, do not an effective VPN make. Indeed, powerful control capabilities are of primary importance in VPN communications, as wide area networking is at best a complicated endeavor. A VPN must include management methods that allow for centralized and regional control over the security devices (and the other networking components) within the network.
3. Management Security: A VPN's management traffic is the most sensitive data flowing in the network. It includes policy table updates, security auditing and logging data, key exchange definitions (elapsed time or bytes sent), and encryption and authentication methodologies. In order to maintain the confidentiality of such information it is important to secure it with no less than the same technologies used for the other forms of VPN traffic. Better still, however, would be to provide a dedicated encryption plus firewall device for the central management station. Such a precaution not only secures management traffic as it traverses the public network, but it also builds a wall between the VPN master manager and personnel residing in his own local network who might seek to undermine the security of the VPN.

The above user needs we can collate with real VPN products (Appendix B, C). It must be built on dedicated hardware platforms, and deliver advanced security features in tamper proof and easily managed solutions. VPN products must provide IPSec network encryption, integrated firewall functions, redundant back-up tunneling, advanced dynamic key management, network address translation (NAT), automatic network topology

learning and IPSec encrypted VPN management traffic. Designed for both large (MFA Central Office) and small (embassy) scale environments, implemented VPNs must come with user-friendly management systems that provide simple and secure pathways (with IPSec encryption and dedicated firewall support) for centralized and regional network management.

As the VPN market begins to mature, we are confident that this demand will be provided by the manufacturers. Ukraine also has companies like "Almaz" that produce appropriate hardware solution for VPN using GOST 28147-89 as an encryption technique.

9. Government Standard of the USSR and Russia GOST 28147-89

The Government Standard of the USSR 28147-89 [13], cryptographic protection for data protection systems, appears to have played a role in the Ukraine similar to that played by the U.S. Data Encryption Standard (FIPS 46). When issued, it bore the minimal classification 'For Official Use', but is now said to be widely available in the Former Soviet Union and elsewhere. In apparent contrast to DES's explicit limitation to unclassified information, the introduction to GOST 28147-89 contains the remark that the cryptographic transformation algorithm "does not place any limitations on the secrecy level of the protected information."

The algorithms are similar in that both operate on 64-bit blocks by successively modifying half of the bits with a function of the other half. Beyond that, the similarity declines and several differences are visible.

- The Soviet System has 32 rounds compare to the 16 of DES.
- Each round is somewhat simpler than a round of DES. In the 'f' function, 32 bits of text are added modulo 32 to 32 bits of key, transformed by a block of eight, 4-bit to 4-bit S-boxes and rotated 11 bits to the left.
- In contrast to DES's meager 56 bits of key, GOST 28147-89 has 256 bits of primary key and 512 bits of secondary key. The secondary key is the block of eight S-boxes, which are specific to individual networks and are not included in the standard.
- In place of complex key schedule of DES, the primary key is divided into eight 32-bit words. For the first twenty-four rounds, these are used cyclically in ascended order. For the last eight, they are used in descending order.

The standard is also somewhat broader than FIPS46. It includes output feedback and cipher feedback modes of operation, both limited to 64-bit blocks, and a mode for producing message authentication codes.

This Standard provides strong encryption and ease of software and hardware implementation. The software network protection driver ensures the transparent modification of the IP-packets within the network with the rate of 500 Kbytes/s (Pentium 166 processor, network rate without driver 900 Kbytes/s). [14]

VI. SECURE MESSAGING

The major benefit of VPN approach is no software or knowledge is required at the users' desktops. All necessary traffic is encrypted and signed at the Ministry level. Therefore, this approach will work regardless of the e-mail and other subsystems in use in the MFA.

In addition, the some VPN products can perform virus checking and content management, to protect organization network from "spam" and Trojan Horses. However it does not provide encryption to the desktop, or address "person to person" authentication issues and it can leave the interior of such networks open to attacks from the inside.

B. MINISTRY TO INDIVIDUALS MESSAGING

By using the secure client software, the Ministry must be able to build secure messaging system between offices and individuals across the Internet. The client software must provide messages encryption using S/MIME, PGP/MIME or other similar protocol. That kind of product may by integrated into the leading e-mail applications as a "plug-in" or be a standalone program. Used in conjunction with the secure mail server it must provide a secure messaging solution between Ministry and individual users.

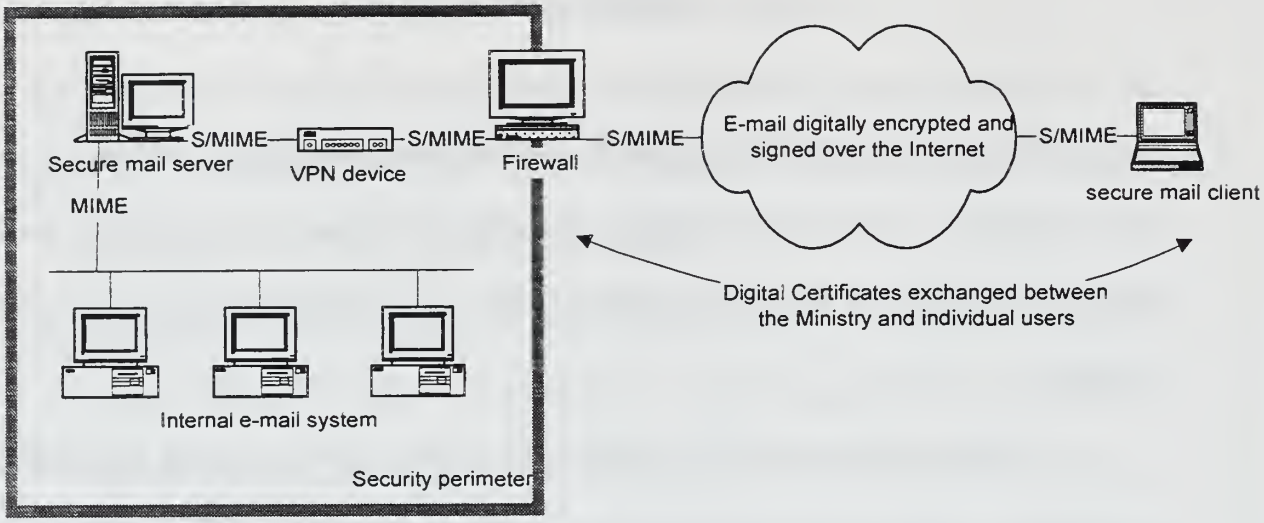

Figure 6. Ministry to individual secure e-mail

In this example, users on the Internet wishing to sign and encrypt e-mail to the Ministry would require the public key of the Ministry. This could be communicated electronically over e-mail, published on a Web Server or stored in an LDAP (Lightweight Directory Access Protocol) directory.

The secure mail server must be able to define policies at the user level. Therefore once it has the public key of a user running the secure client, it can encrypt and sign all e-mail to the user.

This architecture is ideal for an MFA that has a requirement to exchange e-mail securely with delegations, other government, and international organizations, who do not have sufficient amount of users to justify the investment in the VPN or for another reason.

C. PERSON TO PERSON MESSAGING

The secure e-mail client can be used to provide person to person encryption and authentication solutions. For example, software products like PGP from Network Associates Inc. can be used for this purpose and provide a high level of object security. (See Appendix E.) That type of secure client should be deployed within an organization to secure e-mail for senior diplomats, managers, financial officers and other specialists, as well as across the Internet. The main benefits of this solution are high security level for the objects (files, messages, disks, etc.), the elimination of the need to retrain users on a new e-mail package and the retention of the existing e-mail infrastructure

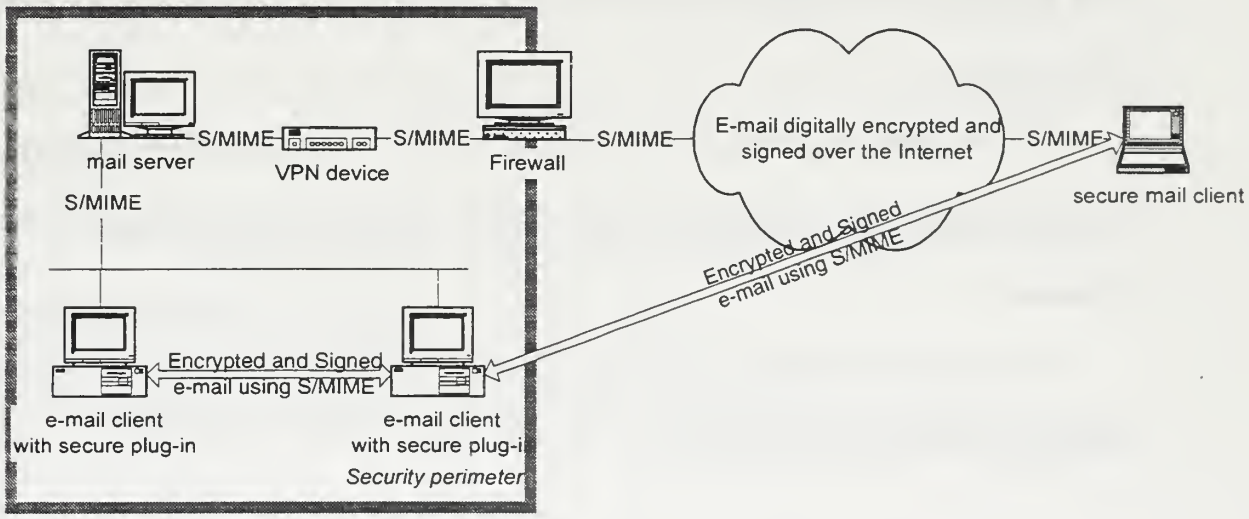

Figure 7. Person to Person secure e-mail

The example above shows two users exchanging encrypted and signed e-mail across the internal e-mail system, and the same users communicating over the Internet to

someone outside the organization. In order for these users to communicate securely, they must first exchange certificates containing each users public key information. These can be exchanged by e-mail and then authenticated by checking the checksum or hash using a secure method e.g. over the telephone.

Alternatively users can have their certificates "certified" by a Trusted Third Party (TTP); this may be an internal Certificate Authority (CA) or an external organization such as Verisign. Using certificates authenticated by a TTP eliminates the need to establish trust on a "one-to-one" basis.

Pros and Cons

The benefit of this approach is it enables secure messaging at the user's desktop. Users are able to store encrypted messages in folders and communicate both internally and externally.

This approach is ideal for communicating with small populations of users, however managing and exchanging digital certificates for larger numbers of users can be impractical.

By using the Certificate server it is possible to deploy person to person secure messaging across the whole Ministry.

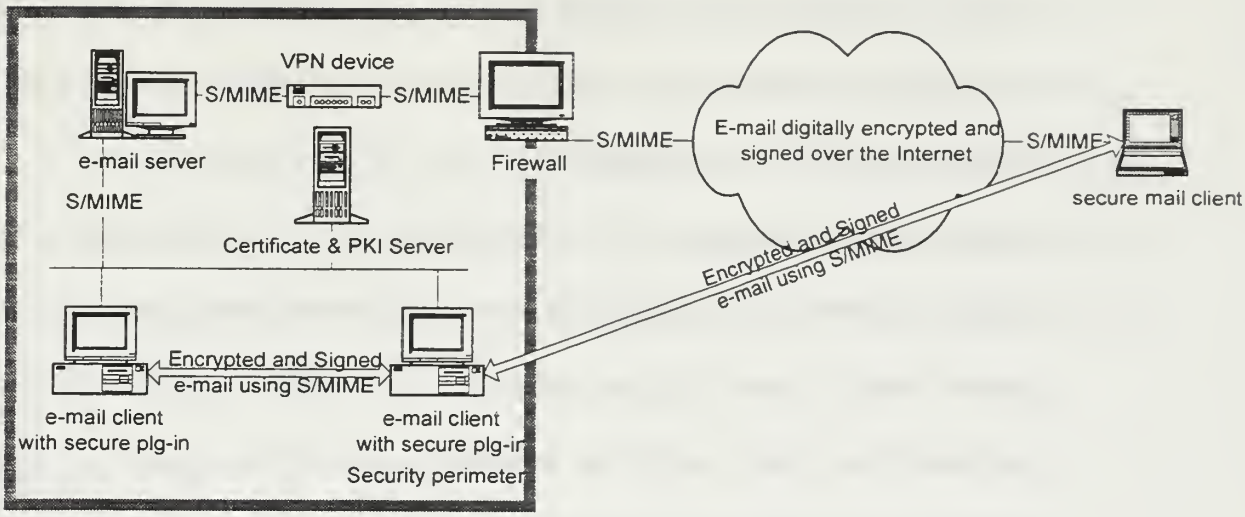

Figure 8. Messaging system with certificate server & PKI

The certificate server provides a central repository for digital certificates and removes the requirement placed on the user to exchange public key information. The clients and mail servers can access the certificate server to obtain up-to-date public key information.

The certificate servers also must provide a direct interface to any Public Key Infrastructure (PKI) that supports X.509 Certificates.

D. SUMMARY OF REQUIREMENTS FOR SECURE E-MAIL SOLUTION

Any secure electronic mail solution must be based upon a robust set of requirements that make it enforceable, manageable, easy-to-use for end-users, interoperable, reliable, and scaleable:

1. Security policies must be enforceable. Secure messaging solution must allow administrators and policy-makers to both define and enforce MFA security

policies for object security. System must allow administrators to mandate virus scanning, content control, access control, encryption, and digital signature policies from a central point of administration.

2. Solution must be ubiquitous. Security solutions are most effective when they apply to everyone in an organization. Secure mail server should intercepts every piece of e-mail or other object and enforces security policies on it. Further, client and server both should support the S/MIME protocol for encryption and digital signature, making them interoperable with millions of other S/MIME-enabled applications (such as Netscape Communicator).
3. Solution must be easy to use for end users. Secure messaging system must be designed as a security overlay to existing e-mail products and technologies. The secure client must natively "plugs in" to existing desktop e-mail clients. With this approach, end users can continue to use the applications they are familiar with, while adding the benefits of secure e-mail. Even better, the secure mail server should be completely transparent to the end user. Its job is to define and enforce e-mail policies, while providing reminders to e-mail users when they are in policy violation.
4. Solution must be modular and interoperable. Secure messaging system must supports major open standards for all elements of the solution, including S/MIME as the secure e-mail protocol, LDAP for the directory/certificate access protocol, and X.509 for digital identification. Additionally, it should supports a wide variety of trust models – including the most flexible choice of certificate

authorities available from a secure application suite. This allows MFA users to combine their preferred e-mail solutions with their preferred certificate authority.

5. Solution must be easy to deploy and manage. Secure messaging system must has both client and server components that have a quick installation, with very few steps to perform before the products are up and running. The server should runs on Windows NT.

VII. NETWORK ARCHITECTURE

A. OVERVIEW

To build an end-to-end networking solution, it is important to consider the three essential building blocks. They include the local area, remote access, and wide area portions of the MFA network. All three of these building blocks play a part in deploying Internet access, intranets, and VPN.

For each of these areas there is three qualities that matter in a network: reliability, usability, and value. To ensure a reliable network, we must determine how robustly it must perform, how resilient and available, and how secure it will be. To have a usable network, it must provide easy installation, operation, and service of the network, all of which can dramatically reduce overall cost of ownership. Value goes beyond the initial purchase price to include how well MFA network adapts to change and therefore protects government investment over time.

B. NETWORK DESIGN

As Figure 9 shows, designing a network is an iterative activity.

The first step for the network design is understands network requirements. There are several methods to obtain this information:

- *User community profiles*--Outline what different user groups require.
- *Interviews, focus group, and surveys*--Build a baseline for implementing a network.

- *Human factor tests*--The most expensive, time consuming method is to conduct a test involving representative users in a lab environment.

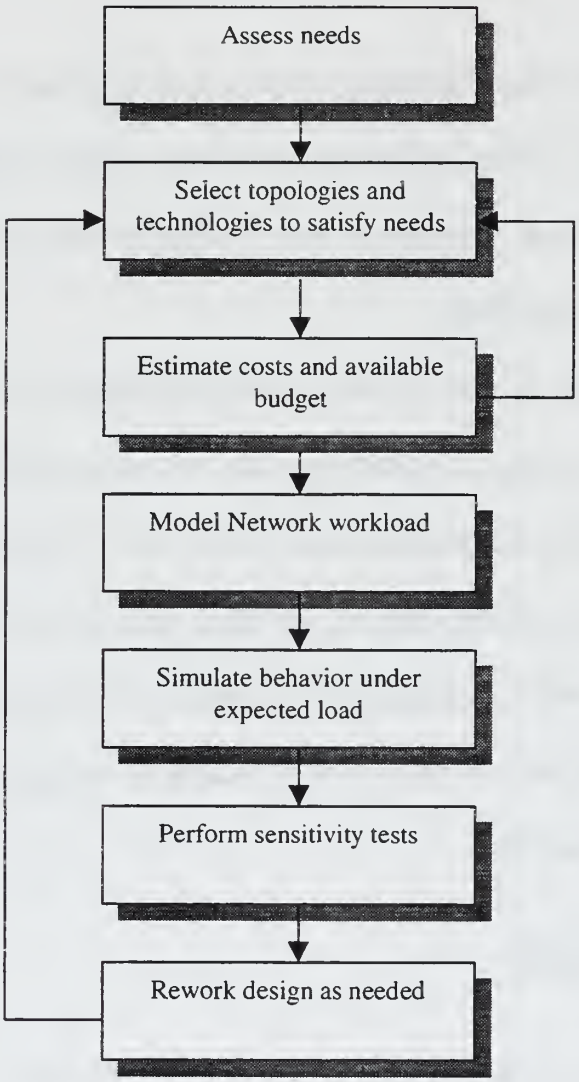

Figure 9. General network design process.

Hierarchical models for network design [15] allows us to develop network and select topologies and technologies in layers. By using layers, we can simplify network

design. Each layer can be focused on specific functions and features. Hierarchical network design includes the following three layers:

- The backbone (core) layer that provides optimal transport between sites.
- The distribution layer that provides policy-based connectivity.
- The local access layer that provides workgroup/user access to the network.

Figure 10 shows a high-level view of the various aspects of a hierarchical network design.

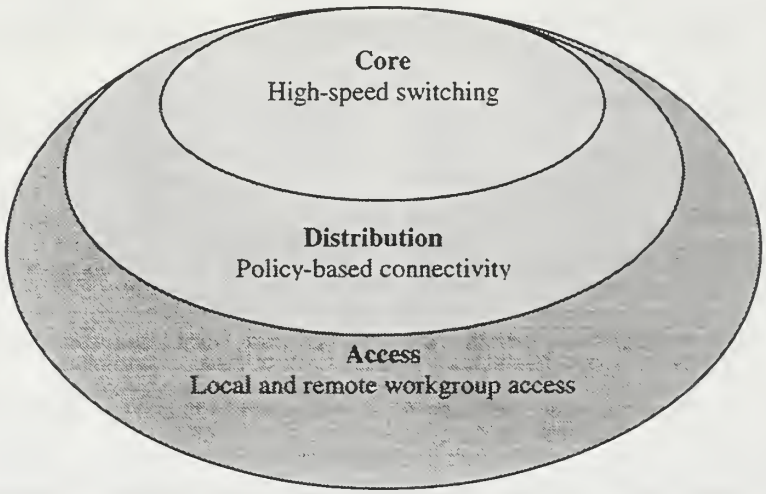

Figure 10. Hierarchical network design model.

The core layer is a high-speed switching backbone and should be designed to switch packets as fast as possible. This layer of the network should not perform any packet manipulation, such as access list and filtering, that would slow down the switching of packets.

The distribution layer of the network provides boundary definition and is a place at which packet manipulation can take place. The main functions of this layer:

- Address or area aggregation.
- Departmental or workgroup access.
- Broadcast/multicast domain definition.
- Virtual LAN routing.
- Security.

This layer provides policy-based connectivity.

The access layer is the point at which local end users are allowed into the network. In the MFA environment, access-layer functions can include following:

- Shared bandwidth.
- Switched bandwidth.
- MAC layer filtering.
- Microsegmentation.

The layers are defined to aid successful network design and to represent functionality that must exist in a network. The instantiation of each layer can be in distinct routers or switches, can be represented by a physical media, can be combined in a single device, or omitted altogether. The way the layers could be implemented depends on the needs of the network being design. We do not have possibility to discuss all phases and details of the network design in this chapter. We just can show an example of the MFA Central Office network diagram and an embassy communication and network diagram. (Figures 11 and 12).

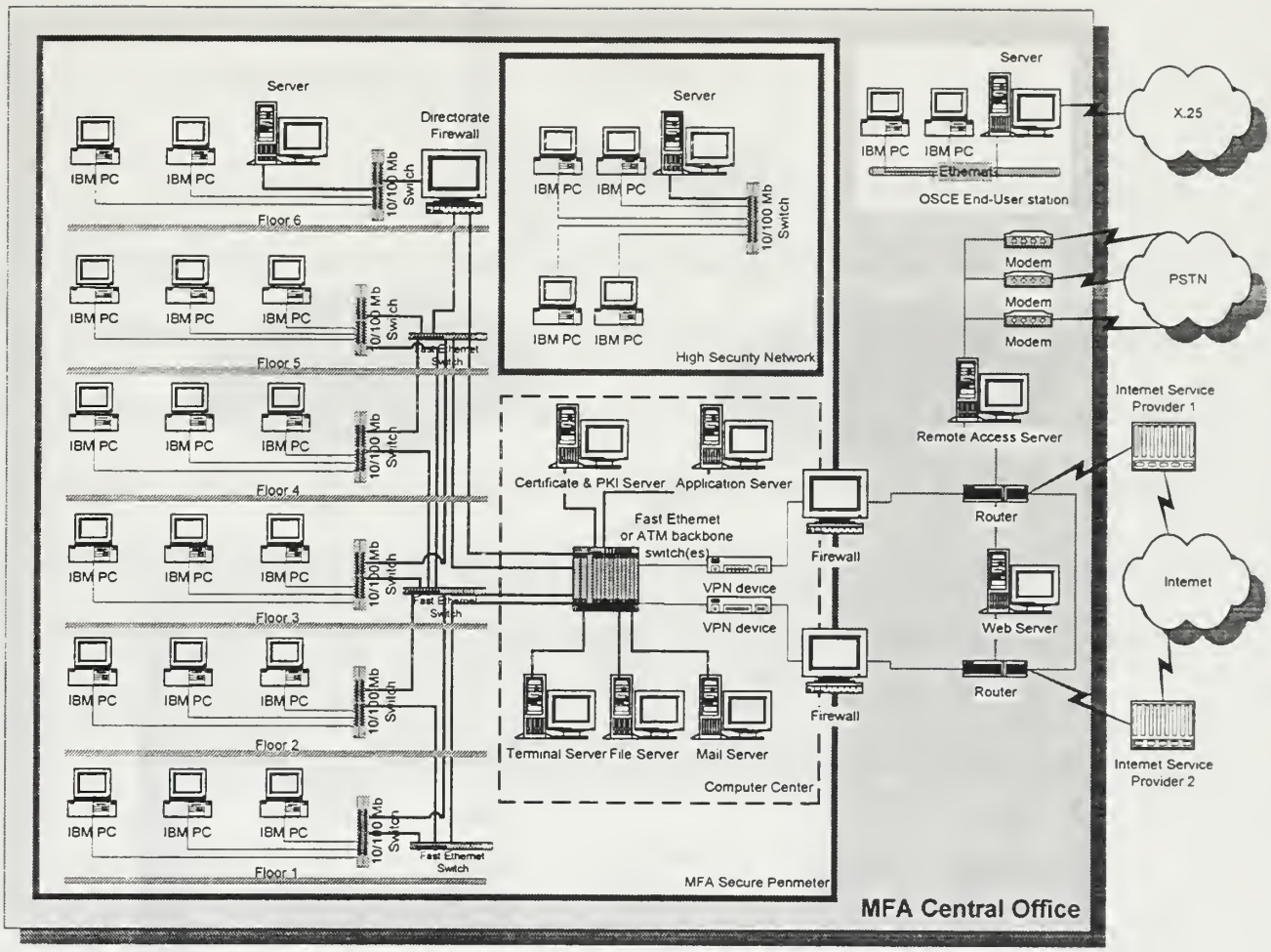

Figure 11. MFA of Ukraine Central Office network diagram.

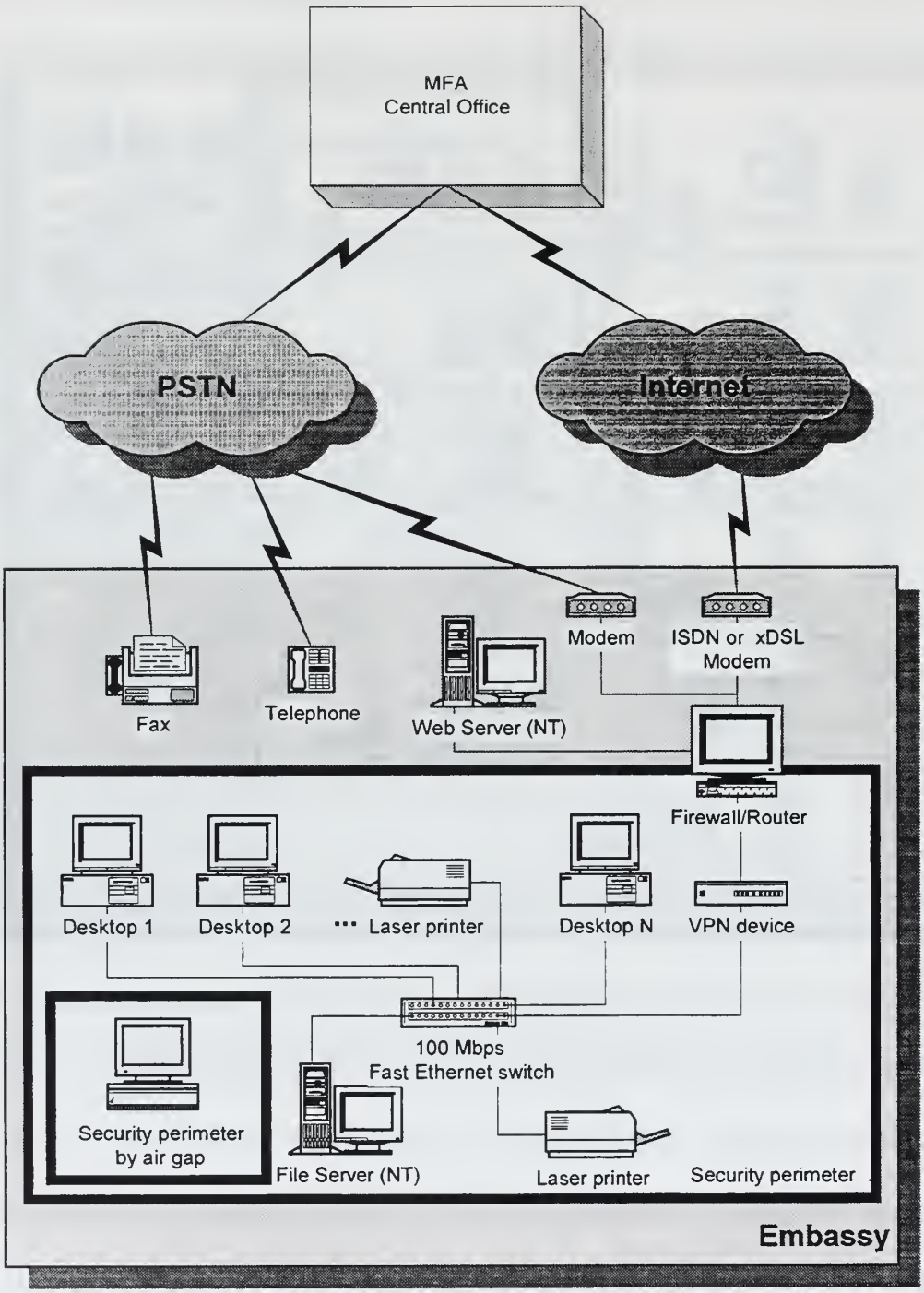

Figure 12. Embassy communication and network diagram

VIII. COMPUTER SECURITY POLICY AND IMPLEMENTATION

A. COMPUTER SECURITY

Computer security refers to the technological safeguards and managerial procedures which can be applied to computer hardware, programs, data, facilities and workplaces to assure the availability, integrity, and confidentiality of computer based resources and to assure that intended functions are performed without harmful side effects. Computer security must be presented in the areas of physical, software, information, and network security as they relate to the security requirements of Information Infrastructure. The intent of this chapter is to discuss the following security objectives:

- Confidentiality of classified or sensitive information handled by the MFA computer system.
- Integrity of information and related processes handled by MFA Information Infrastructure, from its origin through input, processing, and finally the output phase.
- The availability of information when it is needed.
- Accountability of persons accessing the data.

B. THREATS AND CONTROLS

1. Physical Security

Physical security can be divided into two major categories. First are those measures taken to protect against natural disasters such as fires, floods, and power outages/surges. Second are those measures, taken to protect against intruders.

a. Natural Disasters

Threats. The major area of concern for Informational Infrastructure in this area is due to power outages and surges as a result of storms, brownouts, and equipment failure. Damages caused by these types of threats can cause thousands of dollars worth of damage to both the equipment and the information stored on them.

Controls. The following is a list of measures that should be considered to aid in minimizing the effects from these and other natural disasters [16]:

- Mandatory use UPS (Uninterruptible Power Supply) for routers and servers.
- Use surge protectors.
- Schedule frequent backups of diskettes and hard disk drives (where appropriate).
- Save documents being worked on frequently (applies primarily to word processing).
- Locate equipment away from windows.
- Keep equipment elevated to prevent damage due to standing water.

- Use adequate fire protection measures

b. Intruders

Threats. Physical access must be restricted in order to protect data and equipment against common criminals, so-called activists, espionage agents, and trusted persons engaged in any unauthorized acts. Computer systems are an especially attractive target for thieves.

Controls. Due to the current nature of personal computers, physical access control measures are considered to be the best method for denying unauthorized access. The following is a list of measures that should be considered to aid in reducing the threat from intruders:

Place equipment in limited access areas. This includes the space surrounding equipment processing sensitive information that is under sufficient physical and administrative control to preclude an unauthorized entry or compromise.

Ensure systems are not left unattended during normal working hours (i.e.--secured during coffee breaks, lunch breaks, etc.).

- Use sign-in logs for systems used by multiple users.
- Use access rosters of approved users to identify authorized personnel.
- Use physical restraint devices to prevent removal of equipment.
- Ensure that when an office space is vacant during non-duty hours, doors are secured and access is controlled.
- Use a checklist for securing the area at the end of the day.

- Use a device that can be installed in the power circuit to terminate power that can then be physically locked to prevent restoration of power to the equipment.
- Maintain accurate inventories of both hardware and software. These items should be listed by serial or plant property number.

2. Software Security

The Ministry of Foreign Affairs of Ukraine honors all licenses, copyrights, patents, restrictions, terms, and conditions associated with commercial, proprietary computer software.

Personnel are not authorized to copy (other than for backup), modify or transfer purchased computer programs. "Pirating" (making unauthorized copies of software) is a violation of copyright laws, and employees are subject to indictment and conviction if found guilty.

Unauthorized copies are illegal even if they are used only for the government job and are never taken home for personal use.

Threats. A common practice on computer systems is to backup software onto diskettes. The ease with which this is done makes the theft or unauthorized use of government developed or procured software very inviting. The most common threat in this area, especially in Ukraine and other Former Soviet Union countries, is from the user who owns computer system and believes there is nothing wrong with making copies of software packages for their personal use.

Controls. A vast majority of the software being used on personal/desktop computers in the MFA falls into the category of off-the-shelf software.

Most off-the-shelf software is proprietary or licensed and as such may not be distributed or copied without proper authorization. To ensure that government developed software is not misused or stolen and that the MFA does not become liable for improper distribution of commercial software products, the following measures should be adhered to:

- Ensure original (diskette or CD) copies of software products are properly secured and accounted.
- Periodically audit software inventory to verify holdings.
- Ensure all authorized backup copies are properly secured and controlled by a proper authority.
- Ensure users of software products understand they are not allowed to make copies for personal use or distribution by having them sign a document to that effect.

3. Information Security

The safeguarding of sensitive information is the topic of numerous publications and the basis for virtually all computer security requirements [17].

Threats. Information is one of the areas most frequently involved in fraud and abuse cases. Some of the more common threats are: the entering of unauthorized information, manipulation of authorized information, manipulating or improperly using information files and records, and creation of unauthorized files and records.

Controls. Information being processed on Informational Infrastructure in the MFA today covers the spectrum from classified to Sensitive Unclassified and is considered to be a valuable commodity. As such, appropriate measures must be taken to ensure the safeguarding of this information. The following measures, coupled with the ones covered under physical security, should be considered to aid in providing adequate information security:

- Position terminal screens and printers to minimize unauthorized viewing.
- Properly secure the original source material and computer generated output.
- Properly secure the magnetic media (diskettes, tapes, removable hard disks, etc.).
- Encrypt the data.
- Use password protection for sensitive files.
- Ensure removable disks and diskettes are properly marked.
- Use adequate audit trails to track data from the original source documents through its input into the system and its final output or disposition. Audit trails should include information on who was accessing/using the information at any given point during its existence.
- Avoid storing sensitive data on non-removable media such as a desktop computers hard disk, unless the system is located in a controlled space.

4. Environmental Security

Threats. Although the range of environments that computer systems will operate in has expanded greatly, they are still subject to certain types of common environmental hazards.

Some of the more common threats to the computer systems are: bad quality electrical power, smoke from cigarettes, spilled liquids, extreme temperatures, etc.

Controls. Environmental threats are usually well known and easy to counter. Both the manager and user of computer systems should consider the following measures, in conjunction with those measures previously identified, to aid in countering environmental threats:

- All equipment must be earth-grounded.
- Do not operate equipment in temperature and humidity, which are outside of its indicated operating range. These conditions may be checked in the user's manuals.
- Do not eat, drink or smoke in the immediate area of computer system.
- Use antistatic pads and sprays to control harmful static electricity.

5. Network Security

Threats. Network security can be defined by those measures taken to prevent disclosure or modification of information through taps, manipulation of network interfaces, or components, and emanations. Since the MFA needs Internet access and it is not trustworthy, the internal systems are vulnerable to misuse and attack.

Controls. Usage of VPN and secure messaging system, as we discuss earlier, can prevent network information from some form of disclosure or modification. In addition, a firewall as MFA safeguard can be used to control access between internal trusted network and Internet. A firewall is not a single component, it is a strategy for protecting an organization's Internet-reachable resources. A firewall serves as the gatekeeper between the untrusted Internet and the more trusted internal networks.

The main function of a firewall is to centralize access control. Firewalls can also be used to secure segments of an organization's intranet. Firewalls provide several types of protection:

- They can block unwanted traffic.
- They can direct incoming traffic to more trustworthy internal systems.
- They hide vulnerable systems, which cannot easily be secured from the Internet.
- They can log traffic to and from the private network.
- They can hide information like system names, network topology, network device types, and internal user ID's from the Internet.
- They can provide more robust authentication than standard applications might be able to do.

The most sensitive parts of internal network may be protected by air gap.

6. Personnel Security

People are the most serious threat to computers and automated information. The unintentional errors people commit occur more frequently and cause more damage than do deliberate acts of sabotage. Unknowingly, people destroy or damage computers, related equipment, and software. Unwittingly, people enter incorrect data into the computer or erroneously alter data. Although many losses are caused due to unintentional acts, the intentional acts should not be overlooked. People intentionally damage, steal, or knowingly use automated information and computers for their own personal gain. It is important to remember that all security measures are vulnerable to users who have legitimate access.

Threats. Personnel threats are basically internal. People internal to an organization can steal information or other assets for selling or personal use. Although diplomats have usually strong personal ethics, some MFA employee can take and use computer supplies (disks, printer cartridges, paper, etc.). Beyond theft of supplies and equipment is the abuse of assets. Common abuses include using the computer for personal business, browsing, preparing personal use software programs, and creating personnel use information, such as team rosters, scores, and handicaps.

Controls. It is up to the manager to provide leadership and supervision that will instill confidence and promote strong personal ethics among employees. The following recommendations coupled with strong leadership should be considered to aid in providing adequate personnel security [18]:

- Include both the organization's information security policies and the individual's responsibilities in information security training.
- Publicize procedures to report security violations and irregularities.
- Inform staff that unauthorized duplication and use of licensed software violates the law.
- Indoctrinate new employees to their ethical responsibilities.
- Conduct periodic security briefings for all personnel dealing with sensitive information.
- Ensure personnel are aware that they are responsible for the products of the information systems they process.
- After annual security training, require personnel to sign a statement that they understand their information security responsibilities.
- Assign responsibility for the equipment and the information processed on it to users of computer systems.
- Encourage personnel to be involved in risk analysis and contingency planning.
- Be alert to unusual employee behavior -- low morale, refusal to take leave, or personal problems that may indicate vulnerabilities, which could lead to information security problems.

7. Administrative Security

Some of the most frequently overlooked security measures that can be implemented are simple administrative procedures. Although these procedures tend to be simple in nature, they are sometimes the most important ones to enforce.

Managers and users of computer systems should ensure administrative procedures, such as those previously listed and the following, are closely adhered to:

- Conduct periodic inventories of hardware and software products.
- Ensure equipment is appropriately carried on an individual's property account.
- Do not share passwords with anyone else.
- Do not tape passwords to desks, walls, or terminals. Commit it to the memory.
- Establish and enforce password rules and be sure everyone knows them.
- If audit trail printouts are produced, review them regularly and frequently.
- Use a filing system to keep track of removable disks and diskettes.
- Ensure procedures are in place for laptop computers. These procedures should, at a minimum, address:
    1. Conditions under which they may be checked out.
    2. Check in/out procedures and forms.
    3. Traveling safeguards (i.e. - hand carry, do not leave in hotel rooms, airline policies, etc.).

Summary. Information technologies are inherently double-edged swords: they work for the benefit of the good users and provide new potentials for criminal and improper activities. In our case for MFA Information Infrastructure, it is possible to achieve reasonable security, but it is necessary to understand the nature of the vulnerabilities and how to devise strategies for protection.

IX. LEGACY SYSTEM USAGE

A. INTRODUCTION

According to Table 1, almost fifty percent of computers in the Ministry are old 386 and 486 PCs. The necessity of using this heterogeneous computing environment is a fact of life in the organization. The Ukrainian government does not have enough money for replacing old PC with new. Lowering a Total Cost of Ownership (TOC) is a very important issue.

For the effective usage of this legacy hardware, we can deploy the thin-client/server computing model. Under this model, the application execution and data storage occurs on a central server (or servers), and only a thin piece of client software is required at the client system. One way to achieve this server-based application architecture is to re-write enterprise applications. A more practical method is to use universal, thin-client software in conjunction with an application server and a distributed Windows display protocol.

There are several software products for this purpose:

1. IBM's "WorkSpace On-Demand", a thin-client environment based on OS/2 Warp and Java;
2. Microsoft NT Terminal Server 4.0 Edition;
3. WinFrame/MetaFrame software by Citrix Systems Inc., based on Windows NT Terminal Server 4.0;
4. Liftoff 2.1 by New Moon Software Inc.;
5. ALTiS by EPiCON, Inc.

The ALTiS and Liftoff clients run only with standard Microsoft Windows 95 and Windows NT Workstation and cannot be used by legacy desktop computers. "WorkSpace On-Demand" runs only OS/2 server - operation system that MFA does not have. MS Terminal Server cannot work with DOS and UNIX clients and has other limitation.

Therefore, only Citrix MetaFrame server satisfied requirements.

B. THE THIN-CLIENT/SERVER COMPUTING MODEL

MetaFrame is the server-based computing software for the Citrix - Microsoft co-developed Windows NT 4.0 Server, Terminal Server Edition multi-user software.

Thin-client/server computing requires a multi-user operating system. This allows multiple concurrent users to log on and run applications in separate, protected sessions on a single application server. This type of server-based computing model is especially useful for MFA, because it solves the critical application deployment challenges of management, access, performance and security.

The user applications execute on the Terminal Server and are accessible through thin-client software over dial-up, LAN, WAN and Internet connections. The server-based architecture provides users with consistent, high-performance and universal access to any type of application, including DOS, Windows 16, Windows 32 and client/server

programs, regardless of available bandwidth or client hardware. The multi-user application server design provides IS managers with a manageable and cost-effective way to deliver business critical applications. [19]

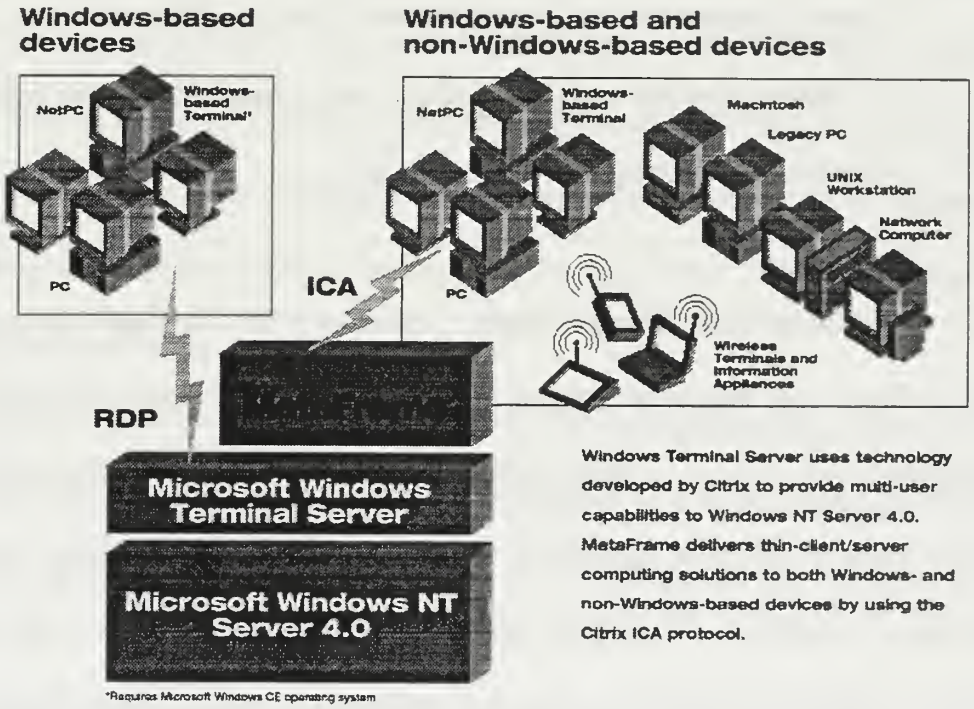

Figure 13. Thin-Client/Server Architecture [20]

Windows Terminal Server is based on Citrix's WinFrame product. Citrix provides a bolt-on, MetaFrame, which adds functionality to Terminal Server, including support for DOS, OS/2, Unix, Java and much more.

With this new software, MFA will be able to:

- Bring thin-client/server computing to heterogeneous computing environments, providing access to Windows-based applications—regardless of client hardware, operating platform, network connection or LAN protocol.
- Offer organization-scale management tools, allowing IT specialists to scale, deploy, manage and support applications from a single location.
- Combine seamless integration of the user's local and remote resources and applications with exceptional performance.

Citrix MetaFrame software based on Windows NT Terminal Server 4.0 offers ways to lower both long-term desktop management costs, as well as short-term capital outlay costs. First, since all applications reside only in a single central place—on the server—there is no client application software that must be developed, installed, or updated on the desktop. This makes application development, rollout, and updates less complex. Second, because all user profile information is stored on the Terminal Server, client desktops are administered centrally by the server. Third, remote administration capabilities further reduce the cost of handling helpdesk calls.

X. CONCLUSIONS AND RECOMMENDATIONS

A. CONCLUSIONS

The construction of an information infrastructure to support Ukrainian diplomacy in the 21st century is one of my most critical and urgent objectives for the Ministry of Foreign Affairs of Ukraine. Providing this technology to the MFA means deploying the modern information networks needed for rapid, secure MFA communications worldwide, strengthening information systems security, and ensuring Year 2000 compliance for critical communication and computer systems.

Thesis research includes a detailed analysis of intranet technology, virtual private networks, secure messaging system and the development of a feasible solution for this government organization. Several major issues were introduced and then discussed in the thesis.

Existing MFA Information Infrastructure was shown to be inadequate to meet organizational needs. Fragmented, unsecured, static, and costly data-storage and limited data-retrieval systems are relics of the past. Information flow, IT department roles and structure should be definitely changed. The technology now exists to transform both the organization and information infrastructure to meet the challenges of operating in a dynamic, uncertain, and complex world. Nowadays question is not "What can technology do?" but "What do we want it to do?"

Another issue discussed an intranet technology overview and possible application of this technology. Intranet may work as a basis for the future of MFA Information

Infrastructure. The benefits, offered by the intranet, include cost savings, minimal training, single source of data, links to outside data sources, and easy management and delivery of information. Intranet implementation may be based on NT 4.0 server platform and Apache 1.3 web server.

The Internet is an almost ideal but not a secure media for information retrieval and exchange between MFA offices around the world. Virtual Private Network systems enable distributed private networks to communicate securely over untrusted, public networks. They encrypt transmitted information with complicated algorithms to hide sensitive data from unauthorized access. The MFA of Ukraine can implement this important part of the information infrastructure using software add-ons to routers, software firewalls with encryption patches, software VPN systems, or dedicated hardware VPNs.

However VPN technology does not provide encryption to the desktop, or address "person to person" authentication issues and it can leave the interior of such networks open to attacks from the inside. By using the secure client software, the MFA can be able to build secure messaging system between offices and individuals across the Internet.

The issue how to build an end-to-end networking solution also was discussed. Network design and requirement steps shown in the thesis can provide feasible cost-effective solution.

The issue how to protect the Information Infrastructure from security threats, without excessively affecting productivity and cost was discussed in terms of a number of

common threats and countermeasures. While no network is 100% safe, a good strategy and vigilant efforts by knowledgeable experts can provide a reasonable tradeoff.

The necessity of using this heterogeneous computing environment is a fact of life in the MFA. Ukrainian government does not have enough money for replacing old PC with new. Lowering a Total Cost of Ownership (TOC) is a very important issue. For the effective usage of this legacy hardware, we can deploy the thin-client/server computing model, based on Citrix MetaFrame software and Windows NT Terminal Server 4.0.

Through use of VPN, secure messaging and intranets, it is increasingly a way of connecting to diplomats, specialists, public and provide basis for development modern Information Infrastructure for the Ministry of Foreign Affairs of Ukraine.

B. RECOMMENDATIONS

In order to design and implement a modern Information Infrastructure, MFA of Ukraine must pass through several steps of system development. These steps are based on each other and can not be omitted.

Phase 1. Decision to invest in a new Information Infrastructure and project initiation.

Activity:

1. Creation of dedicated budget for II development.[3]

[3] The US State Department will invest $118 million in information technology in 1999. (an increase of budget approximately $32 million -- from $86 million in 1998. The State Department has $2.1 billion operating budget in 1999)[21]

2. Increasing number of specialists in the IT department (up to at least 12-15 people)[4].
3. Creation an "IT specialist" posts in the embassies.
4. IT personnel training and education (security officers, network administrators, software engineers, etc.).[5]
5. Cost/benefit and data-flow analysis.

Phase 2. Pilot projects development and testing.

Activity:

1. Design two or three alternative projects for Information Infrastructure development.
2. Pilot projects development for the Intranet, VPN, and secure messaging system.
3. Pilot project testing.
4. Choosing the best IT solution.
5. Security policy development.
6. Network management system development.

Phase 3. Network and desktop hardware deployment and testing.

Activity:

1. Equipment and software purchasing.

---

[4] The US State Department employs a workforce of about 14,000 Americans employees. Approximately 1,450 of them are information technology specialist [21]. Therefore, the ratio is 10:1. For the MFA of Ukraine, this ratio is 1000:1.

[5] In 1999, the US State Department would like to push average IT training to 3 weeks per year [21].

2. The MFA building wiring according to chosen network topology and architecture.
3. Making an additional connection to the Internet.
4. LAN deployment.
5. Network and desktop hardware testing.

Phase 4. Application system deployment and testing.

Activity:

1. Intranet deployment and testing.
2. VPN deployment and testing.
3. Secure messaging system deployment and testing.
4. Legacy support system deployment and testing.
5. The MFA personnel training.

Phase 5. System usage and maintenance.

Activity:

1. System on-going operation and upgrade.
2. Security Policy implementation and audit.

Developing a phased approach to implementation of Information Infrastructure delivers real and tangible benefits to the Ministry, Ukrainian Government and public. Modern information technology can provide for the MFA of Ukraine information superiority achieved through global, affordable, and timely access to reliable and secure information for worldwide decision-making and operation.

APPENDIX A. WEBSERVERS QUICK COMPARISON

Detailed information about "Apache:1.3" and "Internet Information Server 4.0"		
Server	Internet Information Server	Apache
Version	4.0	1.3
Vendor	Microsoft Corp.	The Apache Group
Website of Vendor	www.microsoft.com/iis	www.apache.org
Best Features	Active server pages; support for Microsoft APIs; ODBC driver support.	Fast, supported by public development.
Price	Free with NT 4.0 option pack	Free
Operating System	Windows NT	NetBSD, Digital UNIX, BSDI, AIX, OS/2, SCO, HPUX, Windows NT, Linux, FreeBSD, IRIX, Solaris
Launching and Logging	Can write to multiple logs Log files can be automatically cycled or archived Can generate referer log entries Server can generate non-hit log entries (such as comments) Performance measurement logs CGI scripts can create their own log entries Can serve different directory roots for different IP addresses CERN/NCSA common log format Runs as Windows NT service and/or application Can listen to multiple addresses and ports Normal (hit) log entries can be customized Can track individual users in log Logging with syslog (Unix) or Event Log (Windows NT) Can generate browser log entries	Can write to multiple logs Log files can be automatically cycled or archived Can generate referer log entries Server can generate non-hit log entries (such as comments) CGI scripts can create their own log entries Can serve different directory roots for different IP addresses CERN/NCSA common log format Runs as Windows NT service and/or application Can run from inetd (Unix and OS/2 systems only) Can listen to multiple addresses and ports Normal (hit) log entries can be customized Logging with syslog (Unix) or Event Log (Windows NT) Can generate browser log entries
Header	IIS 4.0	Apache
Protocol Support and Includes	Comes with SNMP agent Supports HTTP/1.1 persistent connections Supports HTTP/1.1 byte ranges Access to server state variables from CGI or other scripting Non-supported methods can invoke a script Select documents based on Accept header Supports HTTP/1.1 PUT Includes based on HTML comments Server can force includes Includes can be based on request headers Select documents based on User-Agent header Has built-in image-map handling Understands full URIs in HTTP/1.1 requests Automatic response to If-Modified-Since Has built-in scripting language	Supports HTTP/1.1 persistent connections Supports HTTP/1.1 byte ranges Access to server state variables from CGI or other scripting Select documents based on Accept header Supports HTTP/1.1 PUT Includes based on HTML comments Server can force includes Includes can be based on request headers Select documents based on User-Agent header Has built-in image-map handling Understands full URIs in HTTP/1.1 requests Automatic response to If-Modified-Since Has built-in scripting language Automatically include any HTTP headers in responses

	Automatically include any HTTP headers in responses Supports Microsoft ISAPI	
Server Side Image Maps	NCSA	NCSA
Security	Integrated certificate server Prohibit access by domain name UID CGI Execution Prohibit access by IP address Prohibit access by user and group Supports S-HTTP Can change user access control list without restarting server Hierarchical permissions for directory-based documents Prohibit access by directory and file Configurable user groups(not just a single user list) Can hide part of a document based on security rules Supports SSL v. 2 Supports SSL v. 3 Supports Set Can require password(Authorization: user) Security rules can be based on URLs	Prohibit access by domain name UID CGI Execution Prohibit access by IP address Prohibit access by user and group Can change user access control list without restarting server Hierarchical permissions for directory-based documents Prohibit access by directory and file Configurable user groups(not just a single user list) Can hide part of a document based on security rules Supports SSL v. 2 Supports SSL v. 3 Can require password(Authorization: user) Security rules can be based on URLs
Default Security Model	Password	Password
Additional Security Features	NT challenge response, X.509 certificate manager, mapped to NT authentication.	
Other Features	GUI-based setup Script or action based on output media type GUI-based maintenance Also serves other TCP protocols Includes user interaction tools Allows non-blocking DNS Multi-Threaded Real-time performance measurement tools Has direct(non-CGI) link to a DBMS Automatic directory tree User directories Search engine Remote maintenance	GUI-based setup Script or action based on output media type Includes full source code for server GUI-based maintenance Also acts as an HTTP proxy server Has a support mailing list Includes user interaction tools Multi-Threaded Has direct(non-CGI) link to a DBMS Automatic directory tree User directories Search engine Proxy server also caches Remote maintenance

APPENDIX B. VPN FEATURES COMPARISON [21]

Products and Services				
VPN Turnkey Solutions				
Company	**Product**	**URL**	**Key features**	**Price**
Ascend Communications	Encrypted VPN Starter Kit	www.ascend.com	Pipeline 220 router, Security Dynamics authentication, IPSec encryption with dynamic firewall technology	$12,000
Bay Networks	NOC 4000 Extranet Access Switch	www.baynetworks.com	Authenticates against internal databases; X.509 certificates, NT Domains; DES, DES-3, RC-4, RSA encryption	$50,000
Extended Systems	ExtendNet VPN	www.extendsys.com	PC-to-LAN server for 10 to 100 remote users via PPTP; supports 40-bit encryption	10 connections, $2,999; 50 connections, $5,999
Fortress Technologies	QuickStart VPN	www.fortresstech.com	Packet compression; dynamic random key exchange; DES, DES-3, or 128-bit IDEA encryption	$10,000
Information Resource Engineering	SafeNet/LAN&trade	www.ire.com	Uses Message Authentication Code, not tokens; FIPS 140-1 certification; DES, IPSec encryption	Varies
Isolation Systems	InfoCrypt Suite	www.isolation.com	Router and firewall; X.509 certificates; Security Dynamics authentication; DES, DES-3 encryption	$6,200 plus $49.95 per client.
Radguard Ltd.	CiPro VPN Solution	www.radguard.com	Hardware certificate authority; ISA/KMP Oakley key exchange; DES, Ipsec encryption	$10,000
Timestep	Permit Enterprise	www.timestep.com	Check Point Software Firewall-1; Permit/Director for management; Permit/Client for remote access	approx. $20,000
VPN Services				
Company	**Product**	**URL**	**Key features**	**Price**
ANS	ANS VPDN	www.ans.net	Supports IDEA, DES, and RC4 data encryption; IPsec promised in the future	Varies
AT&T	WorldNet VPN Service	www.att.com	Guaranteed bandwidth; secure IP addresses, help-desk services for remote users; RADIUS authentication.	From $103/month for 16Kbps access to $2,366/month for 1024Kbps; remote access, $3/hour
CompuServe	IPLink	www.network.compuserve.com	Up to 100 users; supports L2NP, CompuServe Authentication Service; RADIUS authentication; DES encryption	Varies
GTE	Site Patrol Intl	www.bbn.com	Designed for foreign subsidiaries of U.S. companies; authentication using the TIS Gauntlet.	$3,750/month
MCI	InternetMCI VPN	www.networkmci.com)	Combines firewalls, secure remote access, help-desk services, guaranteed completion rates; authentication using CheckPoint SecuRemote tunneling software	Between $2-$6 per hour.
Netcom	Secure Connect	www.netcom.com	Firewall technology from Cisco, Milkyway Networks and Secure Computing when designing a VPN.	Varies

PSInet	intranet	www.psi.net/intranet	Complete custom hardware/sfotware/service solution for private networking between LANs	Varies
Uunet	Extralink	www.uunet.net	Guaranteed connectivity, secure IP addresses; DSS authentication, Diffie-Hellman public-key exchange, L2TP tunneling; DES encryption	Varies

APPENDIX C. SOME VPN SERVERS FEATURES COMPARISON [22]

VPN Server Hardware	ExtendNet VPN v1.4	NetFortress VPN-1 v3.1.1	VSU-1010 v1.1
Vendor	Extended Systems	Fortress Technologies	VPNet Technologies
URL	www.extendedsystems.com	www.fortresstech.com	www.vpnet.com
Phone	(800) 235-7576	(813) 288-7388	(888) 876-3888
Price	$2,999 with 10 clients, $9,999 with 50 clients	$5,995	$4,995*
VPN protocol	PPTP, Layer 2 tunnels	Secure Packet Shield, Layer 3 encrypted sessions	IPsec Layer 3, tunnel & transport mode
Configurations:			
Host-to-LAN	Yes	Yes	Yes
LAN-to-LAN	No	Yes	Yes
VPN granularity of unit tested	Tunnels all traffic sent over adapter interface	Encrypts all traffic sent into a Class B or C subnet	Tunnels all traffic between a defined set of hosts or subnets
LAN Interfaces (number:type)	1: 10Base2, 10BaseT, or 100BaseTX	2: 10BaseT or 10Base2	2: 10BaseT
Simultaneous connections	10-50	1,024	600
Vendor-specified throughput	3.94 Mbps	4.5 Mbps	10 Mbps
User authentication	CHAP, MS-CHAP, PAP, RADIUS	Unit authentication, but no individual user authentication	RADIUS, CHAP, and SecurID (w/ RADIUS)
Data integrity (secure hash)	PPTP packet authentication	Dual checksums (one unencrypted, one encrypted)	MD5
Encryption	40-bit MPPE, 128-bit MPPE*	128-bit IDEA, 56-bit DES**, 168-bit DES3**	56-bit DES, 112-bit DES3*
Key management	MS RAS shared secret; session key changed every 256 packets	Encrypted DH common key and random dynamic key exchange	SKIP
Data compression	MPPC	Lempel-Ziv	Stac Lempel-Ziv
Load balance across ***servers***	No	No	Yes
Tunneled protocols	IP, IPX	IP	IP
Management Interfaces:			
Serial	No	No	Yes
SNMP	Yes	No	Yes
HTTP	Yes	No	No
VPN **Client Software**	**Microsoft *VPN* Adapter**	**NetFortress Remote v1.1**	**VPNremote v2.1**
Price (per client license)	Included in ***server*** price	$99	$99

Platforms	Windows 95 with Microsoft DUN1.2b, Windows NT	Windows 95 with Winsock2	Windows 95
Method of operation	Integrated with DUN	Shim between TCP & NDIS3	Shim between TCP & NDIS
Stacks supported	MSTCP, Novell	MSTCP	MSTCP, OnNet32
***VPN* Management Software**	**InterprEYES v1.5**	**NetFortress Manager v.1.1**	**VPNmanager v2.0**
Price	Included with ***Server***	$1,995	$3,995
Platforms	Windows 95, NT	Windows 95 with Winsock2, Windows NT	Netscape 3.x browser running Java VM
Management interface to ***VPN server***	SNMP (remotely over PPTP)	Secure Packet Shield encrypted session	SSL
Output used to configure ***VPN*** client	None (DUN Client is manually configured)	Centrally-generated signature (executable) files	Centrally-generated configuration files

* ***Features*** corresponding to version sold in US only
** DES and DES3 currently supported by ***VPN***-1 (LAN-to-LAN) but not yet by NetFortress Remote (Host-to-LAN)

APPENDIX D. S/MIME PRODUCTS

S/MIME Product name	Vendor web site
Baltimore Technologies' MailSecure	http://www.baltimore.ie/products/mailsecure/
Entrust	http://www.entrust.com/
Microsoft Outlook and Outlook Express	http://www.microsoft.com/products/prodref/608_ov.htm
Netscape Communicator	http://home.netscape.com/browsers/index.html
OpenSoft ExpressMail	http://www.opensoft.com/products/expressmail/overview/client
SSE TrustedMIME	http://www.sse.ie/trustedmime.html
VeriSign Digital ID	http://www.verisign.com/
WorldTalk	http://www.worldtalk.com/Products/WSS/wss.shtm
NEL Mahobin	http://www.nel.co.jp
RSA BSAFE S/MIME-C Toolkit	http://www.rsa.com/rsa/products/smimec/

APPENDIX E. PGP VERSION 6.0 FEATURES [23]

- Secure Viewer. Secure Viewer is PGP's software solution to protect the private information on your computer screen from interception through electromagnetic radiation—also known as TEMPEST attacks. It is widely known that eavesdroppers, with special equipment, can capture and reconstruct video screen content from radio frequency radiation. When text is encrypted with the Secure Viewer option enabled, the decrypted text is displayed in a special TEMPEST attack prevention font and window that are unreadable to radiation capturing equipment. The Secure Viewer feature allows you to securely view your decrypted text.
- PGPdisk Functionality. PGPdisk functionality is built into PGP version 6.0. PGPdisk is an easy-to-use encryption application that enables you to set aside an area of disk space for storing your sensitive data. • Added Plug-ins. Email plug-ins for Outlook Express and Outlook 98 are included. A Groupwise plugin is available separately.
- Added Plug-ins. Email plug-ins for Outlook Express and Outlook 98 are included. A Groupwise plugin is available separately.
- Photographic User ID. You can add your photograph to your public key. Photo IDs can be signed just like a user ID to provide extra information when verifying the key.
- Secure Communications with the PGP Certificate Server 2.0. PGP provides a secure connection when any query is sent to the server. This secure connection prevents any traffic analysis which might determine the keys you are retrieving from or sending to the server.
- Secure Deletion from the PGP Certificate Server. You can delete or disable your own key on the server by authenticating yourself through Transport Layer Security (TLS).
- PGPkeys Toolbar. An iconic toolbar has been added to PGPkeys for easy access to the most frequently used key management functions.
- Unknown Recipient or Signer Server Lookup. When decrypting or verifying a message, you can automatically perform a server lookup on all the keys which the message is encrypted to or signed by to determine their identity.
- Subkey Management. (Diffie-Hellman/DSS keys only) With the subkey management feature, you can manage your encryption (DH) and signing (DSS) keys separately.
- Signature Reverification. The signatures collected on keys are automatically verified when added to your ring. It is possible, however, whether through data corruption or malicious tampering, for invalid signatures to exist. This new feature allows you to reverify the signatures to ensure that they are valid.
- Signature Expiration. You can create signatures on other keys that will expire after a given date.
- Enhanced Interface. An intuitive toolbar has been added to PGPkeys for easy access to the most frequently used key management functions.

- Improved Application Integration. The PGPtray allows in-place encrypt/decrypt/sign/verify with most applications without the need for an explicit copy and paste by the user.
- Free space Wipe. PGPtools now has the ability to wipe all free space on your disks.
- Enhanced Wiping. Both file and volume wiping now use a significantly enhanced set of patterns over multiple wipes specially tuned for the media types in use by today's computers.
- Key Splitting. Any high security private key can be split into shares among multiple "shareholders" using a cryptographic process known as Blakely-Shamir splitting.
- Designated Revokers. You can now specify that another public key on your keyring is allowed to revoke your key. This can be useful in situations where you are afraid of losing your private key, forgetting your passphrase, or in extreme cases such as a physical incapacity to use the key. In such cases, the third party you designate will be able to revoke your key, send it to the server and it will be just as if you had revoked it yourself.

LIST OF REFERENCES

1. Organization for Security and Co-operation in Europe, OSCE Vienna Document, *Of the negotiations on confidence and security building measures convened in accordance with the relevant provisions of the concluding document of the Vienna meeting of the conference on security and co-operation in Europe,* p.48, 1992.

2. Ministry of Foreign Affairs of Ukraine, *MFA of Ukraine Mission Statement*, 1997.

3. Computer Industry Almanac Inc., "Over 300 Million Internet Users in Year 2000", [http://www.c-i-a.com/199809iu.htm], September 1998.

4. Intranet Design Magazine, "Intranet FAQ", [http://idm.internet.com/ifaq.html], November 1998.

5. Ryan Bernard, Wordmark.Com, Inc., "Building the Corporate Intranet", [http://www.intramark.com/resources/whitepap.htm], March 1998.

6. John Kirch, "Microsoft Windows NT Server 4.0 versus UNIX", [http://www.unix-vs-nt.org/kirch/#web], February 1999.

7. "The definitive guide to HTTP server specs", [http://webcompare.internet.com], February 1999.

8. "Totals for Top Servers Across All Domains", [http://www.netcraft.com/survey/Reports/199812/graphs.html], December 1998.

9. "WebServer Quick Compare", [http://webservercompare.internet.com/cgi-bin/quickcompare.pl], December 1998.

10. Tom Duffy, "Replacing the corporate network with a slice of the Internet isn't for everyone",

[http://www.computerworld.com/home/features.nsf/all/980427intra_main], April 1998.

11. S. Kent and R. Atkinson, "Security architecture for Internet Protocol, RFC 2401", [ftp://ftp.isi.edu/in-notes/rfc2401.txt], November 1998.

12. National Soviet Bureau of Standards, *GOST 28147-89*, 1989.

13. "Universal Software Solution for IP-traffic Protection and Filtering in Real-Time Mode in Public and Corporate Networks", [http://www.infotecs.ru/english], November 1997

14. *Cisco CCIE* Fundamentals*: Network Design and Case Studies*, p. 23, Cisco Systems Inc., 1998.

15. Arthur, E. Hutt, Seymour Bosworth, Douglas B. Hoyt, *Computer security handbook*, 3d ed., p.1-11, John Wiley & Sons, Inc., 1995.

16. D. Russel, G. Gangemi, *Computer Security Basics*, O'Reily & Associates, Inc., 1997

17. Arthur, E. Hutt, Seymour Bosworth, Douglas B. Hoyt, *Computer security handbook*, 3d ed., p.17-20, John Wiley & Sons, Inc., 1995.

18. "Microsoft Windows NT Server, Terminal Server Edition Overview White Paper", [http://www.microsoft.com/ntserver/basics/terminalserver/], January 1999.

19. "Server-based computing software that transforms the way enterprises deploy, manage and access business-critical applications", http://www.citrix.com/products/metaframe.asp], February 1999.

20. Bonnie R. Cohen, "Statement before the Senate Task Force on Function 150", Washington, DC, [http://www.state.gov/www/policy_remarks/1998/ 980917_cohen_function150.html], September 17, 1998.

21. Ted Stevenson, "VPN Products and Services features comparison", [http://www.internetworld.com/print/1998/02/09/iwlabs/19980209-chart.html], December 1998.

22. "Features Comparison - VPN Servers", [http://www.internetworld.com/print/1998/04/06/iwlabs/19980406-vpnchart.html], April 1998.

23. *PGP freeware for Windows 95, 98, and NT. User's Guide Version 6.0*, Network Associates, Inc., 1998.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center 2
   8725 John J. Kingman Road, Ste 0944
   Fort Belvoir, VA 22060-6218

2. Dudley Knox Library 2
   Naval Postgraduate School
   411 Dyer Road
   Monterey, California 93943-5101

3. Professor James Emery, Code SM/SG 1
   Naval Postgraduate School
   Monterey, CA 93943

4. Professor Rex A. Buddenberg Code SM/SG 1
   Naval Postgraduate School
   Monterey, CA 93943

5. Ministry of Foreign Affairs of Ukraine 9
   1 Mykhailivska sq.
   Attn: Oleksiy Illyashov
   Kyiv-18, Ukraine 252018

15 483NPG
TH 3372
10/99 22527-200 NULF

DUDLEY KNOX LIBRARY
3 2768 00366242 0